

Strong Secrecy for Multiple Access Channels

Moritz Wiese and Holger Boche

Technische Universität München

Dedicated to the memory of Rudolf Ahlswede

Abstract. We show strongly secret achievable rate regions for two different wiretap multiple-access channel coding problems. In the first problem, each encoder has a private message and both together have a common message to transmit. The encoders have entropy-limited access to common randomness. If no common randomness is available, then the achievable region derived here does not allow for the secret transmission of a common message. The second coding problem assumes that the encoders do not have a common message nor access to common randomness. However, they may have a conferencing link over which they may iteratively exchange rate-limited information. This can be used to form a common message and common randomness to reduce the second coding problem to the first one. We give the example of a channel where the achievable region equals zero without conferencing or common randomness and where conferencing establishes the possibility of secret message transmission. Both coding problems describe practically relevant networks which need to be secured against eavesdropping attacks.

Contents

1 Introduction	2
2 The Wiretap Multiple-Access Channel	6
2.1 With Common Message	6
2.2 With Conferencing Encoders	8
3 Coding Theorems	10
3.1 For the Wiretap MAC with Common Message	10
3.2 For the Wiretap MAC with Conferencing Encoders	13
4 Proof of Theorem 3.1	15
4.1 Elementary Rate Regions	15
4.2 How to Prove Secrecy	18
4.3 Probabilistic Bounds for Secrecy	19
4.4 Random Coding for the Non-Wiretap MAC with Common Message	36
4.5 Coding	38
4.6 Concluding Steps	42
5 Proof of Theorem 3.5	43
5.1 Elementary Rate Regions	43
5.2 Coding	44

6 Discussion	46
6.1 Conferencing and Secret Transmission	46
6.2 Necessity of Time-Sharing in Random Coding	50
A Proof of Lemma 4.2	51
B Proof of Lemma 4.5	52

1 Introduction

The wiretap Multiple-Access Channel (MAC) combines two areas where Rudolf Ahlswede has made major contributions. In the area of multi-user information theory, he [9] and Liao [25] independently gave one of the first complete characterizations of the capacity region of a multi-user channel – the MAC with one message per sender. Later, Dueck [18] proved the strong converse for the MAC and Ahlswede [10] gave an elementary proof immediately afterwards. Slepian and Wolf generalized the results from [9] and [25] to the case where the senders additionally have a common message [32]. Willems used Slepian and Wolf’s result to derive the capacity region of the MAC with conferencing encoders. This is a MAC without common message, but the encoders can exchange rate-limited information about their messages in an interactive conferencing protocol [38, 39]. The results of Slepian and Wolf as well as Willems’ result were only recently generalized to general compound MACs with partial channel state information in [37], arbitrarily varying MACs with conferencing encoders were treated in [36]. The latter paper made substantial use of techniques developed by Ahlswede for single-sender arbitrarily varying channels in [1–3] and also of his and Cai’s contribution to arbitrarily varying MACs [5].

The other area of Ahlswede’s interest which plays a role in this paper is secrecy and common randomness. Among other problems, he considered together with Csiszár in [6, 7] how a secret key can be shared at distant terminals in the presence of an eavesdropper. Work on secret key sharing aided by public communication goes back to Maurer [28]. The first paper which exploits the statistics of a discrete memoryless channel to establish secret communication is due to Wyner [40]. He considers the wiretap channel, the simplest model of a communication scenario where secrecy is relevant: a sender would like to transmit a message to a receiver over a discrete memoryless channel and transmission is overheard by a second receiver who should be kept ignorant of the message. It was noted by Wyner that a secret key shared at both legitimate terminals is not necessary to establish secret transmission – if the channel statistics are taken into consideration, it is sufficient that the sender randomizes his inputs in order to secure transmission.

Since Wyner discovered this fact, information-theoretic secrecy for message transmission without a key shared between sender and legitimate receiver has been generalized in various directions. The first paper on multi-user information-theoretic security is due to Csiszár and Körner [15]. Here, the second receiver only is a partial eavesdropper: there is a common message intended for both

receivers, but as in the original wiretap channel, an additional private message intended for the first receiver must be kept secret from the second. We come to multiple-access models below. An overview over the area is given in [24].

The original secrecy criterion used in [40] and [15] and in most of the subsequent work until today has become known as the “weak secrecy criterion”. Given a code, it measures the mutual information normalized by the code block-length between the randomly chosen message and the eavesdropper’s output corresponding to the application of the code and transmission over the channel. Maurer introduced the “strong secrecy criterion” in [29] by omitting the normalization. The advantage of this criterion was revealed in [11]: it can be given an operational meaning, i.e. one can specify the attacks it withstands. It is possible to show that if transmission obeys the strong secrecy criterion, then the eavesdropper’s average error tends to one for any decoder it might apply. Translated into practical secrecy schemes, this means that no matter how large the computing power of a possible eavesdropper might be, it will not succeed in breaking the security of this scheme. For the weak criterion, there are still only heuristic argumentations as to why it should be secret. Further secrecy metrics are presented in [12], but without giving them an operational meaning, strong secrecy remains the strongest of these metrics. To our knowledge, there are three different approaches to establishing strong secrecy in a wiretap channel so far [28, 14, 17]. In fact, the last of these approaches also applies to classical-quantum wiretap channels [17] and also was used to give an achievable rate for the classical compound wiretap channel [11].

There exist many MAC models where secrecy is an issue. This may even be the case when there is no eavesdropper, as each encoder might have access to noisy observations of the other sender’s codeword but wants to protect its own message from decoding at the other sender [27, 23, 19]. The case where the encoders have access to generalized feedback but only keep their messages secret from an external eavesdropper is considered in [33]. In the cognitive MAC, only one encoder has a private message, and together, the encoders have a common message. There are again two cases: In the case without an eavesdropper, the encoder without a private message has access to the codeword sent by the other encoder through a noisy channel and must be kept ignorant of the other encoder’s private message [26]. In [31], the cognitive MAC without feedback was investigated where the messages must be kept secret from an eavesdropper and the encoders have unrestricted access to common randomness. All of these papers use the weak secrecy criterion.

The first part of this article generalizes and strengthens the achievability result from [20] where multi-letter characterizations of an achievable region and of an outer bound on the capacity region of a MAC without common message and with an external eavesdropper under the weak secrecy criterion are given. The channel needs to satisfy certain relatively strong conditions for the bounds to work. Extensions to the Gaussian case can be found in [20, 34, 21].

We consider two senders Alice₁ and Alice₂. Each has a private message and together they have a common message. This message triple must be transmitted

to Bob over a discrete memoryless MAC in such a way that Eve who obtains a version of the sent codewords through another discrete memoryless MAC cannot decode the messages. We apply the strong secrecy criterion. In order to find a code which satisfies this criterion, we use Devetak's approach [17], which in the quantum case builds on the Ahlswede-Winter lemma [8] and classically on a Chernoff bound. It is similar to the approach taken in [13]. As the senders have a common message and as the second part of the paper deals with the wiretap MAC with conferencing encoders, we assume that the encoders have access to a restricted amount of common randomness. Common randomness for encoding has so far only been used in [31], but without setting any limitations on its amount. Note that this use of common randomness in order to establish secrecy differs from the use made in [6, 7]. We only obtain an achievable region. In this achievable region it is not possible to transmit a common message if no common randomness is available. Further it is notable that we use random coding and have to apply time-sharing before derandomizing.

The wiretap MAC with common message and common randomness is also needed in the second part of this paper about the wiretap MAC with conferencing encoders. Conferencing was introduced by Willems in [38, 39] and is an iterative protocol for the senders of a MAC to exchange information about their messages. One assumes that the amount of information that is exchanged is rate-limited because otherwise one would obtain a single-encoder wiretap MAC. Willems already used the coding theorem for the MAC with common message to deduce an achievable region for the conferencing MAC. The same can be done for the wiretap MAC with conferencing encoders. More precisely, aside from the senders' private messages, there are no further messages to be transmitted, and no common randomness is available. However, conferencing is used to produce both a common message and common randomness, which allows the reduction. A consequence of the fact that no common message can be transmitted by the wiretap MAC with common message if there is no common randomness is that one has to use conferencing to establish some common randomness if this is supposed to enlarge the achievable region compared to what would be achievable without conferencing. Again, this consequence presumes that the achievable region equals the capacity region even though we cannot prove this.

Information-theoretic security has far-reaching practical consequences. As digital communication replaces more and more of the classical paper-based ways of communication even for the transmission of sensible data, the problem of securing these data becomes increasingly important. Information-theoretic secrecy provides an alternative to the traditional cryptographic approach which bases on the assumption of limited computing power. However, as information-theoretic security uses the imperfections of the channels to secure data, its models must be sufficiently complex to describe realistic scenarios. Our article shows how encoder cooperation can be utilized to secure data. The cooperation of base stations in mobile networks is included in future wireless network standards, and our work can be seen as a contribution to the theoretical analysis of how it fares when it comes to security. But already Csiszár and Körner's paper on the broadcast

channel with confidential messages shows how messages with different secrecy requirements can be combined in one transmission. A more recent example which also applies the strong secrecy criterion is given in [41].

Organization of the paper: The next section introduces the general model of a wiretap MAC and also presents the Willems conferencing protocol. Section 3 contains the two achievability theorems for the wiretap MAC with common message and the wiretap MAC with conferencing encoders.

The common message theorem is treated in the rather long Section 4. First, the regions we claim to be achievable are decomposed into regions whose achievability can be shown more easily. Following Devetak, it is shown that it is sufficient to make Eve's output probability given a message triple almost independent of this triple in terms of variation distance. Then, in the mathematical core of the paper, we derive lower bounds on the randomness necessary to achieve strong secrecy using probabilistic concentration results. Here we also follow Devetak. Having derived these bounds, we finally find a realization of the random codes which defines a good wiretap code.

Section 5 gives the proof of the achievability theorem for the wiretap MAC with conferencing encoders. We again have to decompose the claimed regions into regions whose achievability can be shown more easily. Then we can reduce the problem of achieving a certain rate pair with conferencing to the problem of achieving a certain rate triple by the wiretap MAC with common message more or less in the same way as done by Willems in the non-wiretap situation. Finally, Section 6 shows that conferencing may help in situations where no secret transmission is possible without and that for our approach it is necessary to do the time-sharing within the random coding.

Notation: For sets $\{1, \dots, M\}$, where M is a positive integer, we use the combinatorial shorthand $[M]$. For a real number x we define $[x]_+ := \max\{x, 0\}$.

For any set \mathcal{X} and subset $A \subset \mathcal{X}$ we write $A^c := \mathcal{X} \setminus A$. We let $1_A : \mathcal{X} \rightarrow \{0, 1\}$ be the indicator function of A which takes on the value 1 at $x \in \mathcal{X}$ if and only if $x \in A$. Given a probability space $(\Omega, \mathcal{A}, \mathbb{P})$ we write \mathbb{E} for the expectation corresponding to \mathbb{P} and for $A \in \mathcal{A}$ and a real-valued random variable X we write $\mathbb{E}[X; A] := E[X1_A]$.

The space of probability distributions on the finite set \mathcal{X} is denoted by $\mathcal{P}(\mathcal{X})$. In particular, it contains for every $x \in \mathcal{X}$ the probability measure δ_x defined by $\delta_x(x) = 1$. The product of two probability distributions P and Q is denoted by $P \otimes Q$. A stochastic matrix with input alphabet \mathcal{X} and output alphabet \mathcal{Z} is written as a mapping $W : \mathcal{X} \rightarrow \mathcal{P}(\mathcal{Z})$. The n -fold memoryless extension of a channel $W : \mathcal{X} \rightarrow \mathcal{P}(\mathcal{Z})$ is denoted by $W^{\otimes n}$, so that for $\mathbf{x} = (x_1, \dots, x_n) \in \mathcal{X}^n$ and $\mathbf{z} = (z_1, \dots, z_n) \in \mathcal{Z}^n$,

$$W^{\otimes n}(\mathbf{z}|\mathbf{x}) = \prod_{i=1}^n W(z_i|x_i).$$

We also define for $P \in \mathcal{P}(\mathcal{X})$ and $W : \mathcal{X} \rightarrow \mathcal{P}(\mathcal{Z})$ the probability distribution $P \otimes W \in \mathcal{P}(\mathcal{X} \times \mathcal{Z})$ by $(P \otimes W)(x, z) = P(x)W(z|x)$.

Every measure μ on the finite set \mathcal{X} can be identified with a unique function $\mu : \mathcal{X} \rightarrow [0, \infty]$. Then for any subset $A \subset \mathcal{X}$ we have $\mu(A) = \sum_{x \in A} \mu(x)$. On the set of measures on \mathcal{X} , we define the total variation distance by

$$\|\mu_1 - \mu_2\| := \sum_{x \in \mathcal{X}} |\mu_1(x) - \mu_2(x)|.$$

Given a random variable X living on \mathcal{X} and a $P \in \mathcal{P}(\mathcal{X})$, we mean by $X \sim P$ that P is the distribution of X . Given a pair of random variables (X, Y) taking values in the finite set $\mathcal{X} \times \mathcal{Y}$, we write $P_X \in \mathcal{P}(\mathcal{X})$ for the distribution of X and $P_{X|Y}$ for the conditional distribution of X given Y . We also write $T_{X,\delta}^n \subset \mathcal{X}^n$ for the subset of δ -typical sequences with respect to X and $T_{X|Y,\delta}^n(\mathbf{y}) \subset \mathcal{X}^n$ for the subset of conditionally δ -typical sequences with respect to $P_{X|Y}$ given $\mathbf{y} \in \mathcal{Y}^n$. Given a sequence $\mathbf{x} \in \mathcal{X}^n$ and an $x \in \mathcal{X}$, we let $N(x|\mathbf{x})$ be the number of coordinates of \mathbf{x} equal to x .

For random variables X, Y, Z we write $H(X)$ for the entropy of X , $H(X|Y)$ for the conditional entropy of X given Y , $I(X \wedge Y)$ for the mutual information of X and Y and $I(X \wedge Y|Z)$ for the conditional mutual information of X and Y given Z .

Acknowledgment: We would like to thank A. J. Pierrot for bringing the papers [30] and [42] to our attention. They consider strong secrecy problems in multi-user settings with the help of resolvability theory. In particular, in [42], an achievable region for the wiretap MAC without common message or conferencing is derived.

2 The Wiretap Multiple-Access Channel

The wiretap Multiple-Access Channel (MAC) is described by a stochastic matrix

$$W : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{T} \times \mathcal{Z},$$

where $\mathcal{X}, \mathcal{Y}, \mathcal{T}, \mathcal{Z}$ are finite sets. We write W_b and W_e for the marginal channels to \mathcal{T} and \mathcal{Z} , so e.g.

$$W_b(t|x, y) := \sum_{z \in \mathcal{Z}} W(t, z|x, y).$$

\mathcal{X} and \mathcal{Y} are the finite alphabets of Alice₁ and Alice₂, respectively. \mathcal{T} is the finite alphabet of the receiver called Bob and the outputs received by the eavesdropper Eve are elements of the finite alphabet \mathcal{Z} .

2.1 With Common Message

Let H_C be a nonnegative real number. A wiretap MAC code with common message and blocklength n satisfying the common randomness bound H_C consists

of a stochastic matrix

$$G : [K_0] \times [K_1] \times [K_2] \rightarrow \mathcal{P}(\mathcal{X}^n \times \mathcal{Y}^n)$$

and a decoding function

$$\varphi : \mathcal{T}^n \rightarrow [K_0] \times [K_1] \times [K_2].$$

G is required to have the form

$$G(\mathbf{x}, \mathbf{y} | k_0, k_1, k_2) = \sum_{j \in \mathcal{J}} G_0(j | k_0) G_1(\mathbf{x} | k_0, k_1, j) G_2(\mathbf{y} | k_0, k_2, j),$$

where \mathcal{J} is some finite set and

$$\begin{aligned} G_0 &: [K_0] \rightarrow \mathcal{P}(\mathcal{J}), \\ G_1 &: [K_0] \times [K_1] \times \mathcal{J} \rightarrow \mathcal{P}(\mathcal{X}), \\ G_2 &: [K_0] \times [K_2] \times \mathcal{J} \rightarrow \mathcal{P}(\mathcal{Y}). \end{aligned}$$

Further, G_0 has to satisfy that $H(J | M_0) \leq nH_C$ for M_0 uniformly distributed on $[K_0]$ and $P_{J|M_0} = G_0$. $[K_0]$ is called the set of common messages, $[K_1]$ is the set of Alice₁'s private messages and $[K_2]$ the set of Alice₂'s private messages.

Let M_0, M_1, M_2 be independent random variables uniformly distributed on $[K_0]$, $[K_1]$ and $[K_2]$, respectively. Further, let X^n, Y^n, T^n, Z^n be random variables such that for $(\mathbf{x}, \mathbf{y}, \mathbf{t}, \mathbf{z}) \in \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{T}^n \times \mathcal{Z}^n$

$$\begin{aligned} P_{X^n Y^n | M_0 M_1 M_2}(\mathbf{x}, \mathbf{y} | k_0, k_1, k_2) &= G(\mathbf{x}, \mathbf{y} | k_0, k_1, k_2), \\ P_{T^n Z^n | X^n Y^n M_0 M_1 M_2}(\mathbf{t}, \mathbf{z} | \mathbf{x}, \mathbf{y}, k_0, k_1, k_2) &= W^{\otimes n}(\mathbf{t}, \mathbf{z} | \mathbf{x}, \mathbf{y}). \end{aligned}$$

Then the average error of the code defined above equals

$$\mathbb{P}[\varphi(T^n) \neq (M_0, M_1, M_2)].$$

Definition 2.1. A rate pair $(R_0, R_1, R_2) \in \mathbb{R}_{\geq 0}^3$ is achievable by the wiretap MAC with common message under the common randomness bound $H_C \geq 0$ if for every $\eta > 0$ and every $\varepsilon \in (0, 1)$ and n large there exists a wiretap MAC code with common message and blocklength n satisfying the common randomness bound H_C and

$$\begin{aligned} \frac{1}{n} \log K_\nu &\geq R_\nu - \eta \quad (\nu = 0, 1, 2), \\ \mathbb{P}[\varphi(T^n) \neq (M_0, M_1, M_2)] &\leq \varepsilon, \\ I(Z^n \wedge M_0 M_1 M_2) &\leq \varepsilon. \end{aligned}$$

Remark 2.2. It was shown in [11] that no matter how Eve tries to decode the messages from the Alices, the average error must tend to one. More precisely,

assume that a wiretap code with common message and blocklength n is given, and assume that Eve has a decoding function

$$\chi : \mathcal{Z}^n \rightarrow [K_0] \times [K_1] \times [K_2].$$

Then

$$\mathbb{P}[\chi(Z^n) \neq (M_0, M_1, M_2)] \geq 1 - \varepsilon'$$

for some ε' which tends to zero as ε tends to zero. If ε tends to zero exponentially fast and K_0, K_1, K_2 grow exponentially, then ε' tends to zero at exponential speed.

More generally assume that $f : [K_0] \times [K_1] \times [K_2] \rightarrow [K']$ is a function satisfying $\mathbb{P}[f(M_0, M_1, M_2) = k'] = 1/K'$ for all $k' \in [K']$. Then with the same argument as in [11] one can show that for every function $g : \mathcal{Z}^n \rightarrow [K']$, one has $\mathbb{P}[f(M) \neq g(Z^n)] \geq 1 - 1/K' - \varepsilon'$ for the same ε' as above. That is, even for $K' = 2$, blind guessing is the best way for Eve to estimate $f(M)$. In particular, no subset of the message random variables, like M_0 or (M_1, M_2) , can be reliably decoded by Eve.

2.2 With Conferencing Encoders

In the wiretap MAC with conferencing encoders, Alice₁ and Alice₂ do not have a common message nor common randomness. However before forming their codewords, they may exchange some information about their private messages according to an iterative and randomized “conferencing” protocol whose deterministic form was introduced by Willems [38, 39]. If the respective message sets are $[K_1]$ and $[K_2]$, such a stochastic Willems conference can be described as follows. Let finite sets \mathcal{J}_1 and \mathcal{J}_2 be given which can be written as products

$$\mathcal{J}_\nu = \mathcal{J}_{\nu,1} \times \dots \times \mathcal{J}_{\nu,I} \quad (\nu = 1, 2)$$

for some positive integer I which does not depend on ν . A Willems conferencing stochastic matrix c completely describing such a conference is determined in an iterative manner via sequences of stochastic matrices $c_{1,1}, \dots, c_{1,I}$ and $c_{2,1}, \dots, c_{2,I}$. $c_{1,i}$ describes the probability distribution of what Alice₁ tells Alice₂ in the i -th conferencing iteration given the knowledge accumulated so far at Alice₁. Thus in general, using the notation

$$\bar{\nu} := \begin{cases} 1 & \text{if } \nu = 2, \\ 2 & \text{if } \nu = 1, \end{cases}$$

these stochastic matrices satisfy for $\nu = 1, 2$ and $i = 2, \dots, I$,

$$\begin{aligned} c_{\nu,1} &: [K_\nu] \rightarrow \mathcal{P}(\mathcal{J}_{\nu,1}), \\ c_{\nu,i} &: [K_\nu] \times \mathcal{J}_{\bar{\nu},1} \times \dots \times \mathcal{J}_{\bar{\nu},i-1} \rightarrow \mathcal{P}(\mathcal{J}_{\nu,i}). \end{aligned}$$

The stochastic matrix $c : [K_1] \times [K_2] \rightarrow \mathcal{P}(\mathcal{J}_1 \times \mathcal{J}_2)$ is obtained by setting

$$\begin{aligned} & c(j_{1,1}, \dots, j_{1,I}, j_{2,1}, \dots, j_{2,I} | k_1, k_2) \\ & := c_{1,1}(j_{1,1} | k_1) c_{2,1}(j_{2,1} | k_2) \cdots \\ & \cdots c_{1,I}(j_{1,I} | k_1, j_{2,1}, \dots, j_{2,I-1}) c_{2,I}(j_{2,I} | k_2, j_{1,1}, \dots, j_{1,I-1}). \end{aligned}$$

We denote the \mathcal{J}_1 - and \mathcal{J}_2 -marginals of this stochastic matrix by c_1 and c_2 , so $c_1(j_{1,1}, \dots, j_{1,I} | k_1, k_2)$ is obtained by summing over $j_{2,1}, \dots, j_{2,I}$ and c_2 is obtained analogously.

Now we define a wiretap MAC code with conferencing encoders. It consists of a Willems conferencing stochastic matrix $c : [K_1] \times [K_2] \rightarrow \mathcal{P}(\mathcal{J}_1 \times \mathcal{J}_2)$ as above together with encoding stochastic matrices

$$\begin{aligned} G_1 & : [K_1] \times \mathcal{J}_2 \rightarrow \mathcal{X}^n, \\ G_2 & : [K_2] \times \mathcal{J}_1 \rightarrow \mathcal{Y}^n \end{aligned}$$

and a decoding function

$$\varphi : \mathcal{T}^n \rightarrow [K_1] \times [K_2].$$

$[K_1]$ is the set of Alice₁'s messages and $[K_2]$ is the set of Alice₂'s messages. A pair $(k_1, k_2) \in [K_1] \times [K_2]$ is encoded into the codeword pair $(\mathbf{x}, \mathbf{y}) \in \mathcal{X}^n \times \mathcal{Y}^n$ with probability

$$\sum_{(j_1, j_2) \in \mathcal{J}_1 \times \mathcal{J}_2} c(j_1, j_2 | k_1, k_2) G_1(\mathbf{x} | k_1, j_2) G_2(\mathbf{y} | k_2, j_1). \quad (1)$$

In particular, conferencing generates common randomness. As both c_1 and c_2 may depend on both encoders' messages, the codewords may as well depend on both messages. Thus if conferencing were unrestricted, this would transform the MAC into a single-user wiretap channel with input alphabet $\mathcal{X} \times \mathcal{Y}$. However, Willems introduces a restriction in terms of the blocklength of the code which is used for transmission. For conferencing under conferencing capacities $C_1, C_2 \geq 0$, he requires that for a blocklength- n code, $|\mathcal{J}_1|$ and $|\mathcal{J}_2|$ satisfy

$$\frac{1}{n} \log |\mathcal{J}_\nu| \leq C_\nu \quad (\nu = 1, 2). \quad (2)$$

We also impose this constraint and define a wiretap MAC code with conferencing capacities $C_1, C_2 \geq 0$ to be a wiretap MAC code with conferencing encoders satisfying (2).

Let a wiretap MAC code with conferencing encoders be given and let M_1, M_2 be independent random variables uniformly distributed on $[K_1]$ and $[K_2]$, respectively. Let X^n, Y^n, T^n, Z^n be random variables such that conditional on (M_1, M_2) , the distribution of (X^n, Y^n) is given by (1) and such that

$$P_{T^n Z^n | X^n Y^n M_1 M_2} = W^{\otimes n}.$$

Then the average error of the code defined above equals

$$\mathbb{P}[\varphi(T^n) \neq (M_1, M_2)].$$

Definition 2.3. A rate pair $(R_1, R_2) \in \mathbb{R}_{\geq 0}^3$ is achievable by the wiretap MAC with conferencing encoders at conferencing capacities $C_1, C_2 > 0$ if for every $\eta > 0$ and every $\varepsilon \in (0, 1)$ and for n large there exists a wiretap MAC code with conferencing capacities C_1, C_2 and blocklength n satisfying

$$\begin{aligned} \frac{1}{n} \log K_\nu &\geq R_\nu - \eta \quad (\nu = 1, 2), \\ \mathbb{P}[\varphi(T^n) \neq (M_1, M_2)] &\leq \varepsilon, \\ I(Z^n \wedge M_1 M_2) &\leq \varepsilon. \end{aligned}$$

Remark 2.4. Here again, as in Remark 2.2, the average decoding error for any decoder Eve might apply tends to 1 if the security criterion is satisfied.

3 Coding Theorems

3.1 For the Wiretap MAC with Common Message

Let $H_C \geq 0$ be the common randomness bound. The rate region whose achievability we are about to claim in Theorem 3.1 can be written as the closure of the convex hull of the union of certain rate sets which are parametrized by the elements of a subset Π_{H_C} of the set Π which is defined as follows. Π contains all probability distributions p of random vectors $(U, V_1, V_2, X, Y, T, Z)$ living on sets $\mathcal{U} \times \mathcal{V}_1 \times \mathcal{V}_2 \times \mathcal{X} \times \mathcal{Y} \times \mathcal{T} \times \mathcal{Z}$, where $\mathcal{U}, \mathcal{V}_1, \mathcal{V}_2$ are finite subsets of the integers and where p has the form

$$p = P_U \otimes P_{V_1|U} \otimes P_{V_2|U} \otimes P_{X|V_1} \otimes P_{Y|V_2} \otimes W.$$

Next we define Π_{H_C} . There are four cases altogether, numbered Case 0 to Case 3. Case 0 corresponds to $H_C = 0$ and if $H_C > 0$, then Π_{H_C} has the form $\Pi_{H_C} = \Pi_{H_C}^{(1)} \cup \Pi_{H_C}^{(2)} \cup \Pi_{H_C}^{(3)}$, and each of these subsets corresponds to one of these cases. The one condition all cases have in common is that $I(Z \wedge V_1 V_2) \leq I(T \wedge V_1 V_2)$.

Case 0: If $H_C = 0$ define the set Π_0 as the set of those $p \in \Pi$ where V_1 and V_2 are independent of U (so we can omit U in this case and V_1 and V_2 are independent) and where p satisfies the inequalities

$$I(Z \wedge V_1) \leq I(T \wedge V_1 | V_2), \quad (3)$$

$$I(Z \wedge V_2) \leq I(T \wedge V_2 | V_1). \quad (4)$$

For $p \in \Pi_0$ define the set $\mathcal{R}^{(0)}(p)$ to be the set of nonnegative triples (R_0, R_1, R_2) satisfying

$$\begin{aligned} R_0 &= 0, \\ R_1 &\leq I(T \wedge V_1 | V_2) - I(Z \wedge V_1) - [I(Z \wedge V_2 | V_1) - I(T \wedge V_2 | V_1)]_+, \\ R_2 &\leq I(T \wedge V_2 | V_1) - I(Z \wedge V_2) - [I(Z \wedge V_1 | V_2) - I(T \wedge V_1 | V_2)]_+, \\ R_1 + R_2 &\leq I(T \wedge V_1 V_2) - I(Z \wedge V_1 V_2). \end{aligned}$$

Case 1: $\Pi_{H_C}^{(1)}$ is the set of those $p \in \Pi$ which satisfy $I(Z \wedge U) < H_C$ and

$$I(Z \wedge V_1|U) \leq I(T \wedge V_1|V_2U), \quad (5)$$

$$I(Z \wedge V_2|U) \leq I(T \wedge V_2|V_1U), \quad (6)$$

$$I(Z \wedge V_1V_2|U) \leq I(T \wedge V_1|V_2U) + I(T \wedge V_2|V_1U). \quad (7)$$

Then we denote by $\mathcal{R}^{(1)}(p)$ the set of nonnegative real triples (R_0, R_1, R_2) satisfying

$$\begin{aligned} R_1 &\leq I(T \wedge V_1|V_2U) - I(Z \wedge V_1|U) \\ &\quad - [I(Z \wedge V_2|V_1U) - I(T \wedge V_2|V_1U)]_+, \\ R_2 &\leq I(T \wedge V_2|V_1U) - I(Z \wedge V_2|U) \\ &\quad - [I(Z \wedge V_1|V_2U) - I(T \wedge V_1|V_2U)]_+, \\ R_1 + R_2 &\leq I(T \wedge V_1V_2|U) - I(Z \wedge V_1V_2|U), \\ R_0 + R_1 + R_2 &\leq I(T \wedge V_1V_2) - I(Z \wedge V_1V_2). \end{aligned}$$

Case 2: The conditions for p to be contained in $\Pi_{H_C}^{(2)}$ cannot be phrased as simply as for $\Pi_{H_C}^{(1)}$. Generally, if $p \in \Pi_{H_C}^{(2)}$ then

$$\min\{I(Z \wedge V_1U), I(Z \wedge V_2U)\} < H_C \leq I(Z \wedge V_1V_2).$$

This is sufficient if $I(Z \wedge V_1|V_2U) = I(Z \wedge V_2|V_1U)$. If $I(Z \wedge V_1|V_2U) > I(Z \wedge V_2|V_1U)$ then we additionally require that

$$\begin{aligned} \alpha_0^{(2)} &:= \max \left(\frac{I(Z \wedge V_1U) - H_C}{I(Z \wedge V_1|V_2U) - I(Z \wedge V_2|V_1U)}, 1 - \frac{I(T \wedge V_2|V_1U)}{I(Z \wedge V_2|V_1U)}, 0 \right) \\ &\leq \alpha_1^{(2)} := \min \left(\frac{I(T \wedge V_1|V_2U)}{I(Z \wedge V_1|V_2U)}, \frac{I(T \wedge V_1V_2|U) - I(Z \wedge V_2|V_1U)}{I(Z \wedge V_1|V_2U) - I(Z \wedge V_2|V_1U)}, 1 \right) \end{aligned}$$

whereas if $I(Z \wedge V_1|V_2U) < I(Z \wedge V_2|V_1U)$ then we need

$$\begin{aligned} \alpha_0^{(2)} &:= \max \left(1 - \frac{I(T \wedge V_2|V_1U)}{I(Z \wedge V_2|V_1U)}, \frac{I(T \wedge V_1V_2|U) - I(Z \wedge V_2|V_1U)}{I(Z \wedge V_1|V_2U) - I(Z \wedge V_2|V_1U)}, 0 \right) \\ &\leq \alpha_1^{(2)} := \min \left(\frac{H_C - I(Z \wedge V_1U)}{I(Z \wedge V_2|V_1U) - I(Z \wedge V_1|V_2U)}, \frac{I(T \wedge V_1|V_2U)}{I(Z \wedge V_1|V_2U)}, 1 \right). \end{aligned}$$

In the case of equality, i.e. if $I(Z \wedge V_1|V_2U) = I(Z \wedge V_2|V_1U)$, we define $\mathcal{R}^{(2)}(p)$ as

$$\begin{aligned} R_1 &\leq I(T \wedge V_1|V_2U), \\ R_2 &\leq I(T \wedge V_2|V_1U), \\ R_1 + R_2 &\leq I(T \wedge V_1V_2|U) - I(Z \wedge V_1|V_2U), \\ R_0 + R_1 + R_2 &\leq I(T \wedge V_1V_2) - I(Z \wedge V_1V_2). \end{aligned}$$

If $I(Z \wedge V_1|V_2U) > I(Z \wedge V_2|V_1U)$, we define $\mathcal{R}^{(2)}(p)$ by

$$\begin{aligned} R_1 &\leq I(T \wedge V_1|V_2U) - \alpha_0^{(2)} I(Z \wedge V_1|V_2U), \\ R_2 &\leq I(T \wedge V_2|V_1U) - (1 - \alpha_1^{(2)}) I(Z \wedge V_2|V_1U), \\ R_1 + R_2 &\leq I(T \wedge V_1V_2|U) - \alpha_0^{(2)} I(Z \wedge V_1|V_2U) \\ &\quad - (1 - \alpha_0^{(2)}) I(Z \wedge V_2|V_1U), \end{aligned} \quad (8)$$

$$\begin{aligned} R_1 + \frac{I(Z \wedge V_2|V_1U)}{I(Z \wedge V_1|V_2U)} R_2 &\leq I(T \wedge V_2|V_1U) \\ &\quad + \left(\frac{I(T \wedge V_1|U)}{I(Z \wedge V_1|V_2U)} - 1 \right) I(Z \wedge V_2|V_1U), \\ R_0 + R_1 + R_2 &\leq I(T \wedge V_1V_2) - I(Z \wedge V_1V_2). \end{aligned} \quad (9)$$

The bound (8) on $R_1 + R_2$ can be reformulated as

$$\begin{aligned} R_1 + R_2 &\leq I(T \wedge V_1V_2|U) - I(Z \wedge V_1V_2|U) \\ &\quad + \min \left\{ H_C - I(Z \wedge U), I(Z \wedge V_1|U), \right. \\ &\quad \left. I(T \wedge V_1|V_2U) \left(\frac{I(Z \wedge V_2|V_1U)}{I(Z \wedge V_1|V_2U)} - 1 \right) + I(Z \wedge V_1|U) \right\}, \end{aligned}$$

and if $I(Z \wedge V_2|V_1U) > 0$, we can give the weighted sum bound (9) the almost symmetric form

$$\frac{R_1}{I(Z \wedge V_1|V_2U)} + \frac{R_2}{I(Z \wedge V_2|V_1U)} \leq \frac{I(T \wedge V_1|U)}{I(Z \wedge V_1|V_2U)} + \frac{I(T \wedge V_2|V_1U)}{I(Z \wedge V_2|V_1U)} - 1.$$

For the case that $I(Z \wedge V_1|V_2U) < I(Z \wedge V_2|V_1U)$, we define $\mathcal{R}^{(2)}(p)$ by exchanging the roles of V_1 and V_2 .

Case 3: We define $\Pi_{H_C}^{(3)}$ to be the set of those $p \in \Pi$ with $I(Z \wedge V_1V_2) < H_C$ and for such a p let $\mathcal{R}^{(3)}(p)$ equal

$$\begin{aligned} R_1 &\leq I(T \wedge V_1|V_2U), \\ R_2 &\leq I(T \wedge V_2|V_1U), \\ R_1 + R_2 &\leq I(T \wedge V_1V_2|U), \\ R_0 + R_1 + R_2 &\leq I(T \wedge V_1V_2) - I(Z \wedge V_1V_2). \end{aligned}$$

Theorem 3.1. *For the common randomness bound $H_C = 0$, the wiretap MAC W with common message achieves the set*

$$\text{closure} \left(\text{conv} \left(\bigcup_{p \in \Pi_0} \mathcal{R}^{(0)}(p) \right) \right). \quad (10)$$

If $H_C > 0$, then the closure of the convex hull of the set

$$\bigcup_{p \in \Pi_{H_C}^{(1)}} \mathcal{R}^{(1)}(p) \cup \bigcup_{p \in \Pi_{H_C}^{(2)}} \mathcal{R}^{(2)}(p) \cup \bigcup_{p \in \Pi_{H_C}^{(3)}} \mathcal{R}^{(3)}(p)$$

is achievable.

Remark 3.2. Using the standard Carathéodory-Fenchel technique, one can show that one may without loss of generality assume $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}| + 5$. However, $|\mathcal{V}_1|$ and $|\mathcal{V}_2|$ cannot be bounded in this way, as the application of the Carathéodory-Fenchel theorem does not preserve the conditional independence of V_1 and V_2 . Thus a characterization of the above achievable region involving sets with upper-bounded cardinality is currently not available. As it would be important for an efficient calculation of the achievable region, it still requires further consideration.

Remark 3.3. If no common randomness is available, then no common message can be transmitted.

Remark 3.4. We have $\mathcal{R}^{(1)}(p) \subset \mathcal{R}^{(2)}(p) \subset \mathcal{R}^{(3)}(p)$. This can be seen directly at the beginning of the proof in Subsection 4.1 where we decompose the regions $\mathcal{R}^{(\nu)}(p)$ for $\nu = 1, 2$ into a union of simpler regions.

In particular, if H_C is larger than the capacity of the single-sender discrete memoryless channel W_e with input alphabet $\mathcal{X} \times \mathcal{Y}$ and output alphabet \mathcal{Z} , then $\Pi_{H_C}^{(3)} = \Pi$ and the achievable set equals

$$\text{closure} \left(\text{conv} \left(\bigcup_{p \in \Pi} \mathcal{R}^{(3)}(p) \right) \right).$$

In this case the maximal sum rate equals

$$\mathcal{C} := \max_{p \in \Pi} (I(T \wedge V_1 V_2) - I(Z \wedge V_1 V_2)). \quad (11)$$

This equals the secrecy capacity of the single-sender wiretap channel when Alice₁ and Alice₂ together are considered as one single sender. In order to see this, we have to show that for any pair (V'_1, V'_2) of random variables on any Cartesian product $\mathcal{V}_1 \times \mathcal{V}_2$ of finite sets one can find random variables (V_1, V_2, U) satisfying $P_{UV_1 V_2} = P_U \otimes (P_{V_1|U} \otimes P_{V_2|U})$ and $P_{V_1 V_2} = P_{V'_1 V'_2}$. Given such arbitrary (V'_1, V'_2) as above, just define $U = V'_1$ and $P_{V_1|U} =$ the identity on \mathcal{V}_1 and $P_{V_2|U} = P_{V'_2|V'_1}$. Then a simple calculation shows that the above conditions are satisfied. Thus (11) equals the secrecy capacity of the single-sender wiretap channel with Alice₁ and Alice₂ combined into a single sender. The remaining conditions on R_1 and R_2 formulated in the definition of $\mathcal{R}^{(3)}(p)$ are not concerned with W_e , they are required by the non-wiretap MAC coding theorem applied to W_b .

3.2 For the Wiretap MAC with Conferencing Encoders

For conferencing capacities $C_1, C_2 > 0$, the achievable rate region is parametrized by the members of $\Pi_{C_1+C_2}$. We have Cases 1-3 from the common message part.

Case 1: For $p \in \Pi_{C_1+C_2}^{(1)}$ we define $\mathcal{R}^{(1)}(p, C_1, C_2)$ by

$$\begin{aligned} R_1 &\leq I(T \wedge V_1 | V_2 U) - I(Z \wedge V_1 | U) \\ &\quad - [I(Z \wedge V_2 | V_1 U) - I(T \wedge V_2 | V_1 U)]_+ + C_1 - [I(Z \wedge U) - C_2]_+, \\ R_2 &\leq I(T \wedge V_2 | V_1 U) - I(Z \wedge V_2 | U) \\ &\quad - [I(Z \wedge V_1 | V_2 U) - I(T \wedge V_1 | V_2 U)]_+ + C_2 - [I(Z \wedge U) - C_1]_+, \\ R_1 + R_2 &\leq \min\{I(T \wedge V_1 V_2 | U) + C_1 + C_2, I(T \wedge V_1 V_2)\} - I(Z \wedge V_1 V_2). \end{aligned}$$

Case 2: For $p \in \Pi_{C_1+C_2}^{(2)}$, we set $J_0^{(\alpha)} := \alpha I(Z \wedge V_2 U) + (1 - \alpha) I(Z \wedge V_1 U)$. For $\alpha \in [\alpha_0^{(2)}, \alpha_1^{(2)}]$ define the set $\mathcal{R}_\alpha^{(2)}(p, C_1, C_2)$ by

$$\begin{aligned} R_1 &\leq I(T \wedge V_1 | V_2 U) - \alpha I(Z \wedge V_1 | V_2 U) + C_1 - [J_0^{(\alpha)} - C_2]_+, \\ R_2 &\leq I(T \wedge V_2 | V_1 U) - (1 - \alpha) I(Z \wedge V_2 | V_1 U) + C_2 - [J_0^{(\alpha)} - C_1]_+, \\ R_1 + R_2 &\leq \min\{I(T \wedge V_1 V_2 | U) + C_1 + C_2, I(T \wedge V_1 V_2)\} - I(Z \wedge V_1 V_2). \end{aligned}$$

Then we set

$$\mathcal{R}^{(2)}(p, C_1, C_2) := \bigcup_{\alpha_0^{(2)} \leq \alpha \leq \alpha_1^{(2)}} \mathcal{R}_\alpha^{(2)}(p, C_1, C_2).$$

Case 3: For $p \in \Pi_{C_1+C_2}^{(3)}$ we define $\mathcal{R}^{(3)}(p, C_1, C_2)$ by

$$\begin{aligned} R_1 &\leq I(T \wedge V_1 | V_2 U) + C_1 - [I(Z \wedge V_1 V_2) - C_2]_+, \\ R_2 &\leq I(T \wedge V_2 | V_1 U) + C_2 - [I(Z \wedge V_1 V_2) - C_1]_+, \\ R_1 + R_2 &\leq \min\{I(T \wedge V_1 V_2 | U) + C_1 + C_2, I(T \wedge V_1 V_2)\} - I(Z \wedge V_1 V_2). \end{aligned}$$

Theorem 3.5. For the conferencing capacities $C_1, C_2 > 0$, the wiretap MAC W with conferencing encoders achieves the closure of the convex hull of the set

$$\bigcup_{p \in \Pi_{H_C}^{(1)}} \mathcal{R}^{(1)}(p, C_1, C_2) \cup \bigcup_{p \in \Pi_{H_C}^{(2)}} \mathcal{R}^{(2)}(p, C_1, C_2) \cup \bigcup_{p \in \Pi_{H_C}^{(3)}} \mathcal{R}^{(3)}(p, C_1, C_2).$$

Remark 3.6. Remark 3.2 applies here, too.

Remark 3.7. The stochastic conferencing protocols employed to achieve the sets in Theorem 3.5 are non-iterative. That means that the c we use in the proof have the form

$$c(v_1, v_2 | k_1, k_2) = c_1(v_1 | k_1) c_2(v_2 | k_2).$$

Remark 3.8. If $C_1 = C_2 = 0$, then the maximal rate set whose achievability we can show is (10). Conferencing only enlarges this set in the presence of a wiretapper if it is used to establish common randomness between the encoders. At least this is true for the achievable region we can show, it cannot be verified in general as long as one does not have a converse. The reason is that conferencing generates a common message shared by Alice₁ and Alice₂. As noted in

Remark 3.3, a common message can only be kept secret if common randomness is available. As the Alices do not have common randomness a priori, this also has to be generated by conferencing, so the Willems conferencing protocol has to be stochastic.

Remark 3.9. With the coding method we apply, conferencing may enable secure transmission if this is not possible without. That means that there are wiretap MACs where the achievable region without conferencing as derived in Theorem 3.1 only contains the rate pair $(0, 0)$ whereas it contains non-trivial rate pairs with $C_1, C_2 > 0$. See Section 6 for an example.

Remark 3.10. If C_1, C_2 are sufficiently large, then the maximal achievable sum rate equals the secrecy capacity \mathcal{C} of the single-sender wiretap channel with input alphabet $\mathcal{X} \times \mathcal{Y}$ and channel matrix W , see (11). In fact, this happens if

- 1) $C_1 + C_2$ is strictly larger than the capacity of the single-sender discrete memoryless channel W_e with input alphabet $\mathcal{X} \times \mathcal{Y}$ and output alphabet \mathcal{Z} ,
- 2) $C_1 + C_2 \geq \min_{p \in \Pi^*} I(T \wedge U)$, where Π^* contains those $p \in \Pi$ which achieve \mathcal{C} .

Condition 1) is sufficient to guarantee that \mathcal{C} is achievable by an element of $\Pi_{C_1+C_2}^{(3)}$ which then equals Π , see Remark 3.4. In particular Π^* is nonempty, and 2) ensures that the maximum over Π of the sum rate bounds from $\mathcal{R}^{(3)}(p, C_1, C_2)$ equals \mathcal{C} .

4 Proof of Theorem 3.1

4.1 Elementary Rate Regions

For Cases 0, 1 and 2 we first show the achievability of certain rate regions whose union or convex combination then yields the achievable regions claimed in the theorem.

For Case 0 and 1: We only consider Case 1, Case 0 is analogous. The considerations hold for $I(Z \wedge V_1|U) < I(Z \wedge V_1|V_2U)$ which is equivalent to $I(Z \wedge V_2|U) < I(Z \wedge V_2|V_1U)$. In the case of equality we can prove the achievability of $\mathcal{R}(p)$ directly. Define

$$\alpha_0^{(1)} := \left[\frac{I(T \wedge V_2|V_1U) - I(Z \wedge V_2|V_1U)}{I(Z \wedge V_2|U) - I(Z \wedge V_2|V_1U)} \right]_+,$$

$$\alpha_1^{(1)} := \min \left\{ \frac{I(T \wedge V_1|V_2U) - I(Z \wedge V_1|U)}{I(Z \wedge V_1|V_2U) - I(Z \wedge V_1|U)}, 1 \right\}.$$

Note that conditions (5)-(7) are equivalent to $\alpha_0^{(1)} \leq \alpha_1^{(1)}$. For $\alpha \in [\alpha_0^{(1)}, \alpha_1^{(1)}]$ we define a rate region $\mathcal{R}_\alpha^{(1)}(p)$ by the bounds

$$\begin{aligned} R_1 &\leq I(T \wedge V_1 | V_2 U) - \alpha I(Z \wedge V_1 | V_2 U) - (1 - \alpha) I(Z \wedge V_1 | U), \\ R_2 &\leq I(T \wedge V_2 | V_1 U) - \alpha I(Z \wedge V_2 | U) - (1 - \alpha) I(Z \wedge V_2 | V_1 U), \\ R_1 + R_2 &\leq I(T \wedge V_1 V_2 | U) - I(Z \wedge V_1 V_2 | U), \\ R_0 + R_1 + R_2 &\leq I(T \wedge V_1 V_2) - I(Z \wedge V_1 V_2). \end{aligned}$$

Lemma 4.1. *We have*

$$\mathcal{R}^{(1)}(p) = \bigcup_{\alpha_0^{(1)} \leq \alpha \leq \alpha_1^{(1)}} \mathcal{R}_\alpha^{(1)}(p).$$

Thus if $\mathcal{R}_\alpha^{(1)}(p)$ is an achievable rate region for every $\alpha \in [\alpha_0^{(1)}, \alpha_1^{(1)}]$, then $\mathcal{R}^{(1)}(p)$ is achievable.

For the proof we use the following lemma which is proved in the appendix.

Lemma 4.2. *Assume that $a_1, a_2, b_1, b_2, c, d, r_1, r_2, r_{12}, r_{012}$ are nonnegative reals satisfying*

$$a_1 > b_1, \quad a_2 < b_2, \quad a_1 + a_2 = b_1 + b_2 = c, \quad r_1 + r_2 \geq r_{12}.$$

Let $0 \leq \alpha_0 \leq \alpha_1 \leq 1$. For every $\alpha \in [\alpha_0, \alpha_1]$, let a three-dimensional convex subset \mathcal{K}_α of $\mathbb{R}_{\geq 0}^3$ be defined by

$$\begin{aligned} R_1 &\leq r_1 - \alpha a_1 - (1 - \alpha) b_1, \\ R_2 &\leq r_2 - \alpha a_2 - (1 - \alpha) b_2, \\ R_1 + R_2 &\leq r_{12} - c, \\ R_0 + R_1 + R_2 &\leq r_{012} - d \end{aligned}$$

and assume that $\mathcal{K}_\alpha \neq \emptyset$ for every α . Then

$$\bigcup_{\alpha_0 \leq \alpha \leq \alpha_1} \mathcal{K}_\alpha = \mathcal{K}, \tag{12}$$

where \mathcal{K} is defined by

$$R_1 \leq r_1 - \alpha_0 a_1 - (1 - \alpha_0) b_1, \tag{13}$$

$$R_2 \leq r_2 - \alpha_1 a_2 - (1 - \alpha_1) b_2, \tag{14}$$

$$R_1 + R_2 \leq r_{12} - c, \tag{15}$$

$$R_0 + R_1 + R_2 \leq r_{012} - d. \tag{16}$$

Proof (Lemma 4.1). The proof is a direct application of Lemma 4.2 by setting

$$\begin{aligned} r_1 &= I(T \wedge V_1 | V_2 U), & r_2 &= I(T \wedge V_2 | V_1 U), \\ r_{12} &= I(T \wedge V_1 V_2 | U), & r_{012} &= I(T \wedge V_1 V_2), \\ a_1 &= I(Z \wedge V_1 | V_2 U), & a_2 &= I(Z \wedge V_2 | U), \\ b_1 &= I(Z \wedge V_1 | U), & b_2 &= I(Z \wedge V_2 | V_1 U), \\ \alpha_0 &= \alpha_0^{(1)}, & \alpha_1 &= \alpha_1^{(1)}. \end{aligned}$$

We just need to show that the bounds (13) and (14) coincide with those from the definition of $\mathcal{R}^{(1)}(p)$. This is easy for the case $\alpha_0^{(1)} = 0$ because in that case we have $I(T \wedge V_2|V_1U) \geq I(Z \wedge V_2|V_1U)$ and the positive part in the bound on R_1 in the definition of $\mathcal{R}^{(1)}(p)$ vanishes. Similarly $\alpha_1^{(1)} = 1$ implies $I(T \wedge V_1|V_2U) \geq I(Z \wedge V_1|V_2U)$ and the positive part in the bound on R_2 in the definition of $\mathcal{R}^{(1)}(p)$ vanishes. Now assume that $\alpha_0^{(1)} > 0$. This assumption implies $I(Z \wedge V_2|V_1U) > I(T \wedge V_2|V_1U)$. Thus we obtain for the equivalent of (13)

$$\begin{aligned}
& I(T \wedge V_1|V_2U) - I(Z \wedge V_1|U) \\
& - \frac{I(T \wedge V_2|V_1U) - I(Z \wedge V_2|V_1U)}{I(Z \wedge V_2|U) - I(Z \wedge V_2|V_1U)} (I(Z \wedge V_1|V_2U) - I(Z \wedge V_1|U)) \\
& = I(T \wedge V_1|V_2U) - I(Z \wedge V_1|U) \\
& - \frac{I(T \wedge V_2|V_1U) - I(Z \wedge V_2|V_1U)}{I(Z \wedge V_2|U) - I(Z \wedge V_2|V_1U)} (I(Z \wedge V_2|V_1U) - I(Z \wedge V_2|U)) \\
& = I(T \wedge V_1|V_2U) + I(T \wedge V_2|V_1U) - I(Z \wedge V_1V_2|U) \\
& = I(T \wedge V_1|V_2U) - I(Z \wedge V_1|U) - [I(Z \wedge V_2|V_1U) - I(T \wedge V_2|V_1U)]_+.
\end{aligned}$$

If $\alpha_1^{(1)} < 1$, we obtain the analog for the bound on R_2 . This shows with Lemma 4.2 that $\mathcal{R}^{(1)}(p)$ can be represented as the union of the sets $\mathcal{R}_\alpha^{(1)}(p)$ for $\alpha_0^{(1)} \leq \alpha \leq \alpha_1^{(1)}$. \square

For Case 2: Here we assume that $I(Z \wedge V_1|V_2U) \neq I(Z \wedge V_2|V_1U)$ which is equivalent to $I(Z \wedge V_1U) \neq I(Z \wedge V_2U)$. In the case of equality, the achievability of $\mathcal{R}^{(2)}(p)$ can be shown directly. Define for $\alpha \in [\alpha_0^{(2)}, \alpha_1^{(2)}]$ the rate set $\mathcal{R}_\alpha^{(2)}(p)$ by the conditions

$$\begin{aligned}
R_1 & \leq I(T \wedge V_1|V_2U) - \alpha I(Z \wedge V_1|V_2U), \\
R_2 & \leq I(T \wedge V_2|V_1U) - (1 - \alpha) I(Z \wedge V_2|V_1U), \\
R_1 + R_2 & \leq I(T \wedge V_1V_2|U) - \alpha I(Z \wedge V_1|V_2U) - (1 - \alpha) I(Z \wedge V_2|V_1U), \\
R_0 + R_1 + R_2 & \leq I(T \wedge V_1V_2) - I(Z \wedge V_1V_2).
\end{aligned}$$

Lemma 4.3. *We have that*

$$\mathcal{R}^{(2)}(p) = \bigcup_{\alpha_0^{(2)} \leq \alpha \leq \alpha_1^{(2)}} \mathcal{R}_\alpha^{(2)}(p).$$

In particular, if $\mathcal{R}_\alpha^{(2)}(p)$ is achievable for every $\alpha \in [\alpha_0^{(2)}, \alpha_1^{(2)}]$, then so is $\mathcal{R}^{(2)}(p)$.

Remark 4.4. The similarity between the rate regions for Case 1 and Case 2 becomes clear in these decompositions. The description for Case 2 is more complex because $\alpha_0^{(2)}$ and $\alpha_1^{(2)}$ are defined through three minima/maxima. This is due to

the fact that the sum $\alpha I(Z \wedge V_1|V_2U) + (1 - \alpha)I(Z \wedge V_2|V_1U)$ is not constant in α . Hence the conditions for $\alpha_0^{(2)} \leq \alpha_1^{(2)}$ cannot be reformulated into simple conditions on the corresponding p .

One obtains Lemma 4.3 from the next lemma by making the following replacements:

$$\begin{aligned} r_1 &= I(T \wedge V_1|V_2U), & r_2 &= I(T \wedge V_2|V_1U), \\ r_{12} &= I(T \wedge V_1V_2|U), & r_{012} &= I(T \wedge V_1V_2), \\ a &= I(Z \wedge V_1|V_2U), & b &= I(Z \wedge V_2|V_1U), \\ c &= I(Z \wedge V_1V_2), \\ \alpha_0 &= \alpha_0^{(2)}, & \alpha_1 &= \alpha_1^{(2)}. \end{aligned}$$

Lemma 4.5. *Let $r_1, r_2, r_{12}, r_{012}, a, b, c$ be nonnegative reals with $\max(r_1, r_2) \leq r_{12} \leq r_1 + r_2$. Let $\alpha_0, \alpha_1 \in [0, 1]$ be given such that for every $\alpha \in [\alpha_0, \alpha_1]$ the set \mathcal{K}_α defined by*

$$\begin{aligned} R_1 &\leq r_1 - \alpha a, \\ R_2 &\leq r_2 - (1 - \alpha)b, \\ R_1 + R_2 &\leq r_{12} - \alpha a - (1 - \alpha)b, \\ R_0 + R_1 + R_2 &\leq r_{012} - c \end{aligned}$$

is nonempty. If $a \leq b$, the convex hull of the union of these sets is given by the set \mathcal{K} which is characterized by

$$0 \leq R_1 \leq r_1 - \alpha_0 a, \tag{17}$$

$$0 \leq R_2 \leq r_2 - (1 - \alpha_1)b, \tag{18}$$

$$R_1 + R_2 \leq r_{12} - \alpha_1 a - (1 - \alpha_1)b, \tag{19}$$

$$bR_1 + aR_2 \leq r_{12}a + r_1(b - a) - ab, \tag{20}$$

$$R_0 + R_1 + R_2 \leq r_{012} - c. \tag{21}$$

If $a > b$, the convex hull of the union of the sets \mathcal{K}_α is given by analogous bounds where a and b are exchanged in (20).

The proof of Lemma 4.5 can be found in the appendix.

4.2 How to Prove Secrecy

Proving secrecy using Chernoff-type concentration inequalities (see Subsection 4.3) is the core of Devetak's approach to the wiretap channel [17]. Due to the multi-user structure of the inputs of the wiretap MAC, we need several such Chernoff-type inequalities basing on each other compared to the one used by Devetak (actually an application of the Ahlswede-Winter lemma). However, once these are established, the way of obtaining secrecy is exactly the same as presented by Devetak. With the help of the inequalities one obtains a code with

stochastic encoding and a measure ϑ (not necessarily a probability measure!) such that for all k_0, k_1, k_2

$$\|P_{Z^n|M_0=k_0, M_1=k_1, M_2=k_2} - \vartheta\| \leq \frac{\varepsilon}{2}. \quad (22)$$

Given this, we now derive an upper bound on $I(Z^n \wedge M_0 M_1 M_2)$, where the random triple (M_0, M_1, M_2) is uniformly distributed on the possible input message triples and Z^n represents the output received by Eve. Observe that

$$\begin{aligned} & I(Z^n \wedge M_0 M_1 M_2) \\ &= \frac{1}{K_0 K_1 K_2} \sum_{k_0, k_1, k_2} (H(Z^n) - H(Z^n | M_0 = k_0, M_1 = k_1, M_2 = k_2)). \end{aligned} \quad (23)$$

By [16, Lemma 2.7], every summand on the right-hand side is upper-bounded by $\varepsilon_{k_0 k_1 k_2} \log(|\mathcal{Z}|^n / \varepsilon_{k_0 k_1 k_2})$ if

$$\varepsilon_{k_0 k_1 k_2} := \|P_{Z^n} - P_{Z^n|M_0=k_0, M_1=k_1, M_2=k_2}\| \leq \frac{1}{2}.$$

But due to (22),

$$\begin{aligned} & \|P_{Z^n} - P_{Z^n|M_0=k_0, M_1=k_1, M_2=k_2}\| \\ & \leq \|P_{Z^n} - \vartheta\| + \|\vartheta - P_{Z^n|M_0=k_0, M_1=k_1, M_2=k_2}\| \\ & \leq \frac{1}{K_0 K_1 K_2} \sum_{\tilde{k}_0, \tilde{k}_1, \tilde{k}_2} \|P_{Z^n|M_0=\tilde{k}_0, M_1=\tilde{k}_1, M_2=\tilde{k}_2} - \vartheta\| + \frac{\varepsilon}{2} \\ & \leq \varepsilon. \end{aligned}$$

Thus if ε tends to zero exponentially in blocklength, then (23) is upper-bounded by $\varepsilon \log(|\mathcal{Z}|^n / \varepsilon)$ which tends to zero in n .

4.3 Probabilistic Bounds for Secrecy

In this subsection we define the random variables from which we will build a stochastic wiretap code in Subsection 4.5. For this family of random variables we prove several Chernoff-type estimates which will serve to find a code satisfying (22). For Case 3, two such estimates are sufficient, Case 0 and 2 require three and Case 1 requires four. Within each case, one deals with the joint typicality of the inputs at Alice₁ and Alice₂, and the other estimates base on each other. This is due to the complex structure of our family of random variables. Still, all the cases are nothing but a generalization of Devetak's approach taken in [17]. For each case, we first show the probabilistic bounds in one paragraph and then in another paragraph how to achieve (22) from those bounds.

Let $p = P_U \otimes P_{X|U} \otimes P_{Y|U} \otimes W \in \Pi$, i.e. p is the distribution of a random vector (U, X, Y, T, Z) . The auxiliary random variables V_1 and V_2 will be introduced later in the usual way of prefixing a channel as a means of additional

randomization. Let $\delta > 0$ and define for any n

$$\begin{aligned} P_U^n(\mathbf{u}) &:= \frac{P_U^{\otimes n}(\mathbf{u})}{P_U^{\otimes n}(T_{U,\delta}^n)} & (\mathbf{u} \in T_{U,\delta}^n), \\ P_{X|U}^n(\mathbf{x}|\mathbf{u}) &:= \frac{P_{X|U}^{\otimes n}(\mathbf{x}|\mathbf{u})}{P_{X|U}^{\otimes n}(T_{X|U,\delta}^n(\mathbf{u})|\mathbf{u})} & (\mathbf{x} \in T_{X|U,\delta}^n(\mathbf{u}), \mathbf{u} \in T_{U,\delta}^n), \\ P_{Y|U}^n(\mathbf{y}|\mathbf{u}) &:= \frac{P_{Y|U}^{\otimes n}(\mathbf{y}|\mathbf{u})}{P_{Y|U}^{\otimes n}(T_{Y|U,\delta}^n(\mathbf{u})|\mathbf{u})} & (\mathbf{y} \in T_{Y|U,\delta}^n(\mathbf{u}), \mathbf{u} \in T_{U,\delta}^n). \end{aligned}$$

Let L_0, L_1, L_2 be positive integers. We define L_0 independent families of random variables $(U^{l_0}, \mathcal{F}_{l_0})$ as follows. U^{l_0} is distributed according to P_U^n . We let $\mathcal{F}_{l_0} := \{X^{l_0 l_1}, Y^{l_0 l_2} : l_1 \in [L_1], l_2 \in [L_2]\}$ be a set of random variables which are independent given U^{l_0} and which satisfy $X^{l_0 l_1} \sim P_{X|U}^n(\cdot | U^{l_0})$ and $Y^{l_0 l_2} \sim P_{Y|U}^n(\cdot | U^{l_0})$. Finally we define

$$\mathcal{F} := \bigcup_{l_0 \in [L_0]} (U^{l_0}, \mathcal{F}_{l_0}). \quad (24)$$

Throughout the section, let a small $\varepsilon > 0$ be fixed. The core of the proofs of all the lemmas of this subsection is the following Chernoff bound, see e.g. [4].

Lemma 4.6. *Let $b > 0$ and $0 < \varepsilon < 1/2$. For an independent sequence of random variables Z_1, \dots, Z_L with values in $[0, b]$ with $\mu_l := \mathbb{E}[Z_l]$ and with $\mu := \frac{1}{L} \sum_l \mu_l$ one has*

$$\mathbb{P} \left[\frac{1}{L} \sum_{l=1}^L Z_l > (1 + \varepsilon) \mu \right] \leq \exp \left(-L \cdot \frac{\varepsilon^2 \mu}{2b \ln 2} \right)$$

and

$$\mathbb{P} \left[\frac{1}{L} \sum_{l=1}^L Z_l < (1 - \varepsilon) \mu \right] \leq \exp \left(-L \cdot \frac{\varepsilon^2 \mu}{2b \ln 2} \right).$$

In order to obtain useful bounds in the following we collect here some well-known estimates concerning typical sets, see e.g. [16, Lemma 17.8]. Let (A, B) be a random pair on the finite Cartesian product $\mathcal{A} \times \mathcal{B}$. Let $\xi, \zeta > 0$. Then there exists a $\tilde{c} = \tilde{c}(|\mathcal{A}|, |\mathcal{B}|) > 0$ such that for sufficiently large n

$$P_{B|A}^{\otimes n}(T_{B|A,\zeta}^n(\mathbf{a})^c | \mathbf{a}) \leq 2^{-n\tilde{c}\zeta^2}. \quad (25)$$

Further there is a $\tau = \tau(P_{AB}, \xi, \zeta)$ with $\tau \rightarrow 0$ as $\xi, \zeta \rightarrow 0$ such that

$$P_{B|A}^{\otimes n}(\mathbf{b} | \mathbf{a}) \leq 2^{-n(H(B|A) - \tau)} \quad \text{if } \mathbf{a} \in T_{A,\xi}^n, \mathbf{b} \in T_{B|A,\zeta}^n, \quad (26)$$

and that for n sufficiently large,

$$\begin{aligned} |T_{A,\xi}^n| &\leq 2^{n(H(A)+\tau)}, \\ |T_{B|A,\zeta}^n(\mathbf{a})| &\leq 2^{n(H(B|A)+\tau)} \quad \text{if } \mathbf{a} \in T_{A,\xi}^n. \end{aligned} \quad (27)$$

We set

$$c := \tilde{c}(|\mathcal{U}||\mathcal{X}||\mathcal{Y}||\mathcal{Z}|),$$

this is the minimal \tilde{c} we will need in the following.

Bounds for Case 0 and 1: Let L_0, L_1, L_2 be arbitrary. Due to their conditional independence, the $X^{l_0 l_1}$ and $Y^{l_0 l_2}$ cannot be required to be jointly conditionally typical given U^{l_0} . However, the next lemma shows that most of them are jointly conditionally typical with high probability.

Lemma 4.7. *For $(l_0, l_2) \in [L_0] \times [L_2]$, let the event $A_*^{(1)}(l_0, l_2)$ be defined by*

$$\begin{aligned} &A_*^{(1)}(l_0, l_2) \\ &:= \{|\{l_1 \in [L_1] : X^{l_0 l_1} \in T_{X|YU,\delta}^n(Y^{l_0 l_2}, U^{l_0})\}| \geq (1-\varepsilon)(1-2 \cdot 2^{-nc\delta^2})L_1\}. \end{aligned}$$

Then

$$\mathbb{P}[A_*^{(1)}(l_0, l_2)^c] \leq \exp\left(-L_1 \cdot \frac{\varepsilon^2(1-2 \cdot 2^{-nc\delta^2})}{2 \ln 2}\right).$$

Proof. Let $\mathbf{u} \in T_{U,\delta}^n$ and $\mathbf{y} \in T_{Y|U,\delta}^n(\mathbf{u})$. We first condition on the event $\{Y^{l_0 l_2} = \mathbf{y}, U^{l_0} = \mathbf{u}\}$. Due to (25), we have

$$\begin{aligned} &\mathbb{P}[X^{11} \notin T_{X|YU,\delta}^n(\mathbf{y}, \mathbf{u}) | Y^{l_0 l_2} = \mathbf{y}, U^{l_0} = \mathbf{u}] \\ &= \frac{1}{P_{X|U}^{\otimes n}(T_{X|U,\delta}^n(\mathbf{u})|\mathbf{u})} \sum_{\mathbf{x} \in T_{X|U,\delta}^n(\mathbf{u}) \setminus T_{X|YU,\delta}^n(\mathbf{y}, \mathbf{u})} P_{X|U}^{\otimes n}(\mathbf{x}|\mathbf{u}) \\ &\leq \frac{1}{P_{X|U}^{\otimes n}(T_{X|U,\delta}^n(\mathbf{u})|\mathbf{u})} \sum_{\mathbf{x} \notin T_{X|YU,\delta}^n(\mathbf{y}, \mathbf{u})} P_{X|YU}^{\otimes n}(\mathbf{x}|\mathbf{y}, \mathbf{u}) \\ &\leq \frac{2^{-nc\delta^2}}{1-2^{-nc\delta^2}}. \end{aligned}$$

In particular,

$$\mu := \mathbb{P}[X^{11} \in T_{X|YU,\delta}^n(\mathbf{y}, \mathbf{u}) | Y^{11} = \mathbf{y}, U^1 = \mathbf{u}] \geq 1-2 \cdot 2^{-nc\delta^2}.$$

Therefore

$$\begin{aligned} &\mathbb{P}[A_*^{(1)}(l_0, l_2)^c | Y^{l_0 l_2} = \mathbf{y}, U^{l_0} = \mathbf{u}] \\ &\leq \mathbb{P}\left[\sum_{l_1} 1_{T_{X|YU,\delta}^n(\mathbf{y}, \mathbf{u})}(X^{l_0 l_1}) \leq (1-\varepsilon)\mu L_1 \middle| Y^{l_0 l_2} = \mathbf{y}, U^{l_0} = \mathbf{u}\right], \end{aligned}$$

which by Lemma 4.6 can be bounded by

$$\exp\left(-L_1 \cdot \frac{\varepsilon^2 \mu}{2 \ln 2}\right) \leq \exp\left(-L_1 \cdot \frac{\varepsilon^2(1 - 2 \cdot 2^{-nc\delta^2})}{2 \ln 2}\right).$$

This completes the proof as this bound is independent of (\mathbf{y}, \mathbf{u}) . \square

Lemma 4.7 is not needed for a single sender. As we cannot guarantee the joint conditional typicality of both senders' inputs, we need to introduce an explicit bound on the channel transition probabilities. This is done in the set $E_1^{(1)}$. Then we prove three lemmas each of which exploits one of the three types of independence contained in \mathcal{F} . Altogether these lemmas provide lower bounds on L_0, L_1, L_2 which if satisfied allow the construction of a wiretap code satisfying (22). Let

$$E_1^{(1)}(\mathbf{u}, \mathbf{x}, \mathbf{y}) := \{\mathbf{z} \in T_{Z|YU, 2|\mathcal{X}|\delta}^n(\mathbf{y}, \mathbf{u}) : W_e^{\otimes n}(\mathbf{z}|\mathbf{x}, \mathbf{y}) \leq 2^{-n(H(Z|XY) - f_2(\delta))}\},$$

where $f_2(\delta) = \tau(P_{UXYZ}, 3\delta, \delta)$ (see (26)). Let

$$\vartheta_{\mathbf{u}\mathbf{y}}^{(1)}(\mathbf{z}) := \mathbb{E}[W_e^{\otimes n}(\mathbf{z}|X^{11}, \mathbf{y}) 1_{E_1^{(1)}(\mathbf{u}, X^{11}, \mathbf{y})}(\mathbf{z}) | U^1 = \mathbf{u}]$$

and for

$$F_1^{(1)}(\mathbf{u}, \mathbf{y}) := \{\mathbf{z} \in T_{Z|YU, 2|\mathcal{X}|\delta}^n(\mathbf{y}, \mathbf{u}) : \vartheta_{\mathbf{u}\mathbf{y}}^{(1)}(\mathbf{z}) \geq \varepsilon |T_{Z|YU, 2|\mathcal{X}|\delta}^n(\mathbf{y}, \mathbf{u})|^{-1}\}$$

define

$$\hat{\vartheta}_{\mathbf{u}\mathbf{y}}^{(1)} := \vartheta_{\mathbf{u}\mathbf{y}}^{(1)} \cdot 1_{F_1^{(1)}(\mathbf{u}, \mathbf{y})}, \quad E_2^{(1)}(\mathbf{u}, \mathbf{x}, \mathbf{y}) := E_1^{(1)}(\mathbf{u}, \mathbf{x}, \mathbf{y}) \cap F_1^{(1)}(\mathbf{u}, \mathbf{y}).$$

Lemma 4.8. *For every $\mathbf{z} \in \mathcal{Z}^n$ and $(l_0, l_2) \in [L_0] \times [L_2]$, let $A_1^{(1)}(l_0, l_2, \mathbf{z})$ be the event that*

$$\frac{1}{L_1} \sum_{l_1} W_e^{\otimes n}(\mathbf{z}|X^{l_0 l_1}, Y^{l_0 l_2}) 1_{E_2^{(1)}(U^{l_0}, X^{l_0 l_1}, Y^{l_0 l_2})}(\mathbf{z}) \in [(1 \pm \varepsilon) \hat{\vartheta}_{U^{l_0} Y^{l_0 l_2}}^{(1)}(\mathbf{z})].$$

Then

$$\mathbb{P}[A_1^{(1)}(l_0, l_2, \mathbf{z})^c] \leq 2 \exp\left(-L_1 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge X|YU) + f_1(\delta) + f_2(\delta))}}{2 \ln 2}\right)$$

for $f_1(\delta) = \tau(P_{UYZ}, 2\delta, 2|\mathcal{X}|\delta)$ and n sufficiently large.

Proof. For $\mathbf{u} \in T_{U, \delta}^n$ and $\mathbf{y} \in T_{Y|U, \delta}^n(\mathbf{u})$ we condition on the event $\{Y^{l_0 l_2} = \mathbf{y}, U^{l_0} = \mathbf{u}\}$. The conditional expectation of the bounded conditionally i.i.d. random variables

$$W_e^{\otimes n}(\mathbf{z}|X^{l_0 l_1}, \mathbf{y}) 1_{E_2^{(1)}(\mathbf{u}, X^{l_0 l_1}, \mathbf{y})}(\mathbf{z}) \leq 2^{-n(H(Z|XY) - f_2(\delta))} \quad (l_1 \in [L_1])$$

is $\hat{\vartheta}_{\mathbf{u}\mathbf{y}}^{(1)}(\mathbf{z})$. We use Lemma 4.6, the definition of $F_1^{(1)}(\mathbf{u}, \mathbf{y})$, and (28) to obtain for n sufficiently large

$$\begin{aligned} & \mathbb{P}[A_1^{(1)}(l_0, l_2, \mathbf{z})^c | Y^{l_0 l_2} = \mathbf{y}, U^{l_0} = \mathbf{u}] \\ & \leq 2 \exp \left(-L_1 \cdot \frac{\varepsilon^2 \hat{\vartheta}_{\mathbf{u}\mathbf{y}}^{(1)}(\mathbf{z}) 2^{n(H(Z|XY) - f_2(\delta))}}{2 \ln 2} \right) \\ & \leq 2 \exp \left(-L_1 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge X|YU) + f_1(\delta) + f_2(\delta))}}{2 \ln 2} \right). \end{aligned}$$

This bound is uniform in \mathbf{u} and \mathbf{y} , so the proof is complete. \square

For the next lemma, define

$$\vartheta_{\mathbf{u}}^{(1)}(\mathbf{z}) := \mathbb{E}[W_e^{\otimes n}(\mathbf{z}|X^{11}, Y^{11}) 1_{E_2^{(1)}(\mathbf{u}, X^{11}, Y^{11})}(\mathbf{z}) | U^1 = \mathbf{u}].$$

Further let

$$F_2^{(1)}(\mathbf{u}) := \{\mathbf{z} \in T_{Z|U, 3|\mathcal{Y}||\mathcal{X}|\delta}^n(\mathbf{u}) : \vartheta_{\mathbf{u}}^{(1)}(\mathbf{z}) \geq \varepsilon |T_{Z|U, 3|\mathcal{Y}||\mathcal{X}|\delta}^n(\mathbf{u})|^{-1}\}$$

and

$$\hat{\vartheta}_{\mathbf{u}}^{(1)} = \vartheta_{\mathbf{u}}^{(1)} \cdot 1_{F_2^{(1)}(\mathbf{u})}, \quad E_0^{(1)}(\mathbf{u}, \mathbf{x}, \mathbf{y}) := E_2^{(1)}(\mathbf{u}, \mathbf{x}, \mathbf{y}) \cap F_2^{(1)}(\mathbf{u}, \mathbf{y}).$$

Lemma 4.9. *For every $\mathbf{z} \in \mathcal{Z}^n$ and $l_0 \in [L_0]$, let $A_2^{(1)}(l_0, \mathbf{z})$ be the event*

$$\frac{1}{L_1 L_2} \sum_{l_1 l_2} W_e^{\otimes n}(\mathbf{z}|X^{l_0 l_1}, Y^{l_0 l_2}) 1_{E_0^{(1)}(U^{l_0}, X^{l_0 l_1}, Y^{l_0 l_2})}(\mathbf{z}) \in [(1 \pm 3\varepsilon) \hat{\vartheta}_{U^{l_0}}^{(1)}(\mathbf{z})].$$

Then for ε sufficiently small and n sufficiently large,

$$\begin{aligned} \mathbb{P}[A_2^{(1)}(l_0, \mathbf{z})^c] & \leq 2|\mathcal{Y}|^n \exp \left(-L_1 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge X|YU) + f_1(\delta) + f_2(\delta))}}{2 \ln 2} \right) \\ & \quad + 2 \exp \left(-L_2 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge Y|U) + f_1(\delta) + f_4(\delta))}}{4 \ln 2} \right), \end{aligned}$$

where $f_4(\delta) = \tau(P_{UZ}, \delta, 3|\mathcal{Y}||\mathcal{X}|\delta)$.

Proof. Let $\mathbf{u} \in T_{U, \delta}^n$. We define the set $B_{\mathbf{u}} \subset (T_{X|U, \delta}^n(\mathbf{u}))^{L_1}$ as

$$\begin{aligned} & \bigcap_{\mathbf{y} \in T_{Y|U, \delta}^n(\mathbf{u})} \left\{ (\mathbf{x}^1, \dots, \mathbf{x}^{L_1}) \in (T_{X|U, \delta}^n(\mathbf{u}))^{L_1} : \right. \\ & \quad \left. \frac{1}{L_1} \sum_{l_1} W_e^{\otimes n}(\mathbf{z}|\mathbf{x}^{l_0 l_1}, \mathbf{y}) 1_{E_0^{(1)}(\mathbf{u}, X^{l_0 l_1}, \mathbf{y})}(\mathbf{z}) \in [(1 \pm \varepsilon) \hat{\vartheta}_{\mathbf{u}\mathbf{y}}^{(1)}(\mathbf{z})] \right\}. \end{aligned}$$

One has

$$\begin{aligned}
& \mathbb{P}[A_2^{(1)}(l_0, \mathbf{z})^c | U^{l_0} = \mathbf{u}] \\
& \leq \mathbb{P}[\{(X^{l_0 1}, \dots, X^{l_0 L_1}) \notin B_{\mathbf{u}}\} | U^{l_0} = \mathbf{u}] \\
& \quad + \sum_{(\mathbf{x}^1, \dots, \mathbf{x}^{L_1}) \in B_{\mathbf{u}}} \mathbb{P}[A_2^{(1)}(l_0, \mathbf{z})^c | X^{l_0 1} = \mathbf{x}^1, \dots, X^{l_0 L_1} = \mathbf{x}^{L_1}, U^{l_0} = \mathbf{u}] \\
& \quad \cdot \mathbb{P}[X^{l_0 1} = \mathbf{x}^1, \dots, X^{l_0 L_1} = \mathbf{x}^{L_1} | U^{l_0} = \mathbf{u}].
\end{aligned}$$

From the proof of Lemma 4.8 it follows that

$$\begin{aligned}
& \mathbb{P}[\{(X^{l_0 1}, \dots, X^{l_0 L_1}) \notin B_{\mathbf{u}}\} | U^{l_0} = \mathbf{u}] \\
& \leq 2|\mathcal{X}|^n \exp\left(-L_1 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge X | YU) + f_1(\delta) + f_2(\delta))}}{2 \ln 2}\right), \quad (29)
\end{aligned}$$

which gives a bound independent of \mathbf{u} . Now let $(\mathbf{x}^1, \dots, \mathbf{x}^{L_1}) \in B_{\mathbf{u}}$. By (25) and (26),

$$\begin{aligned}
\hat{\vartheta}_{\mathbf{u}\mathbf{y}}^{(1)}(\mathbf{z}) &= \mathbb{E}[W_e^{\otimes n}(\mathbf{z} | X^{11}, \mathbf{y}) 1_{E_2^{(1)}(\mathbf{u}, X^{11}, \mathbf{y})}(\mathbf{z}) | U^1 = \mathbf{u}] \\
&\leq \mathbb{E}[W_e^{\otimes n}(\mathbf{z} | X^{11}, \mathbf{y}) | U^1 = \mathbf{u}] \\
&\leq \frac{1}{P_{X|U}^{\otimes n}(T_{X|U, \delta}^n(\mathbf{u}) | \mathbf{u})} (P_{Z|YU})^{\otimes n}(\mathbf{z} | \mathbf{y}, \mathbf{u}) \\
&\leq (1 - 2^{-nc\delta^2})^{-1} 2^{-n(H(Z|YU) - f_1(\delta))}.
\end{aligned}$$

Hence the random variables

$$\tilde{W}_{\mathbf{u}\mathbf{z}}^{(1)}(l_0, l_2) := \frac{1}{L_1} \sum_{l_1} W_e^{\otimes n}(\mathbf{z} | \mathbf{x}^{l_1}, Y^{l_0 l_2}) 1_{E_0^{(1)}(\mathbf{u}, \mathbf{x}^{l_1}, Y^{l_0 l_2})}(\mathbf{z}) \quad (l_2 \in [L_2]),$$

which are independent conditional on $\{U^{l_0} = \mathbf{u}\}$, are upper-bounded by

$$\frac{(1 + \varepsilon)}{(1 - 2^{-nc\delta^2})} \cdot 2^{-n(H(Z|YU) - f_1(\delta))}.$$

For their conditional expectation we have

$$\begin{aligned}
\mu_{l_0 l_2} &:= \mathbb{E}[\tilde{W}_{\mathbf{u}\mathbf{z}}^{(1)}(l_0, l_2) | U^{l_0} = \mathbf{u}] \\
&\in [(1 \pm \varepsilon) \mathbb{E}[\hat{\vartheta}_{\mathbf{u}Y^{l_0 l_2}}^{(1)}(\mathbf{z}) | U^1 = \mathbf{u}]] = [(1 \pm \varepsilon) \hat{\vartheta}_{\mathbf{u}}^{(1)}(\mathbf{z})].
\end{aligned}$$

Thus their arithmetic mean $\bar{\mu} = (1/L_2) \sum_{l_2} \mu_{l_0 l_2}$ must also be contained in $[(1 \pm \varepsilon) \hat{\vartheta}_{\mathbf{u}}^{(1)}(\mathbf{z})]$. Applying Lemma 4.6, we conclude

$$\begin{aligned} & \mathbb{P}[A_2^{(1)}(l_0, \mathbf{z})^c | X^{l_0 1} = \mathbf{x}^1, \dots, X^{l_0 L_1} = \mathbf{x}^{L_1}, U^{l_0} = \mathbf{u}] \\ &= \mathbb{P}\left[\frac{1}{L_2} \sum_{l_2} \tilde{W}_{\mathbf{uz}}^{(1)}(l_0, l_2) \notin [(1 \pm 3\varepsilon) \hat{\vartheta}_{\mathbf{u}}^{(1)}(\mathbf{z})] \middle| U^{l_0} = \mathbf{u}\right] \\ &\leq \mathbb{P}\left[\frac{1}{L_2} \sum_{l_2} \tilde{W}_{\mathbf{uz}}^{(1)}(l_0, l_2) \notin [(1 \pm \varepsilon) \bar{\mu}] \middle| U^{l_0} = \mathbf{u}\right] \\ &\leq 2 \exp\left(-L_2 \cdot \frac{\varepsilon^2 (1 - 2^{-nc\delta^2}) 2^{n(H(Z|YU) - f_1(\delta))} (1 - \varepsilon) \hat{\vartheta}_{\mathbf{u}}^{(1)}(\mathbf{z})}{2(1 + \varepsilon) \ln 2}\right). \end{aligned}$$

Due to the definition of $F_2^{(1)}(\mathbf{u})$ and to (28), this is smaller than

$$2 \exp\left(-L_2 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge Y|U) + f_1(\delta) + f_4(\delta))}}{4 \ln 2}\right) \quad (30)$$

if ε is sufficiently small and n is sufficiently large, giving a bound independent of \mathbf{u} and $\mathbf{x}^1, \dots, \mathbf{x}^{L_1}$. Adding the bounds (29) and (30) concludes the proof. \square

The next lemma is only needed in Case 1. Let $A_2^{(1)}(\mathbf{z}) := A_2^{(1)}(1, \mathbf{z}) \cap \dots \cap A_2^{(1)}(L_0, \mathbf{z})$. For every \mathbf{z} , we then define a new probability measure by $\hat{\mathbb{P}}_{\mathbf{z}}^{(1)} := \mathbb{P}[\cdot | A_2^{(1)}(\mathbf{z})]$. With $\vartheta^{(1)}(\mathbf{z}) := \hat{\mathbb{E}}_{\mathbf{z}}^{(1)}[\hat{\vartheta}_{U^1}^{(1)}(\mathbf{z})]$ define

$$F_0^{(1)} := \{\mathbf{z} \in T_{Z,4|\mathcal{Y}||\mathcal{X}||\mathcal{U}|\delta}^n : \vartheta^{(1)}(\mathbf{z}) \geq |T_{Z,4|\mathcal{Y}||\mathcal{X}||\mathcal{U}|\delta}^n|^{-1}\}$$

and $\hat{\vartheta}^{(1)} := \vartheta^{(1)} \cdot 1_{F_0^{(1)}}$.

Lemma 4.10. *Let $\mathbf{z} \in F_0^{(1)}$ and let $A_0^{(1)}(\mathbf{z})$ be the event that*

$$\frac{1}{L_0 L_1 L_2} \sum_{l_0, l_1, l_2} W_e^{\otimes n}(\mathbf{z} | X^{l_0 l_1}, Y^{l_0 l_2}) 1_{E_0^{(1)}(U^{l_0}, X^{l_0 l_1}, Y^{l_0 l_2})}(\mathbf{z}) \in [(1 \pm 5\varepsilon) \hat{\vartheta}^{(1)}(\mathbf{z})].$$

Then for $f_6(\delta) = \tau(P_Z, 4|\mathcal{Y}||\mathcal{X}||\mathcal{U}|\delta, \delta)$, sufficiently small ε and n sufficiently large,

$$\begin{aligned} & \mathbb{P}[A_0^{(1)}(\mathbf{z})^c] \\ &\leq 2L_0 |\mathcal{Y}|^n \exp\left(-L_1 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge X|YU) + f_1(\delta) + f_2(\delta))}}{2 \ln 2}\right) \\ &\quad + 2L_0 \exp\left(-L_2 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge Y|U) + f_1(\delta) + f_4(\delta))}}{4 \ln 2}\right) \\ &\quad + 2 \exp\left(-L_0 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge U) + f_4(\delta) + f_6(\delta))}}{4 \ln 2}\right). \end{aligned}$$

Proof. We have

$$\mathbb{P}[A_0^{(1)}(\mathbf{z})^c] \leq \hat{\mathbb{P}}_{\mathbf{z}}^{(1)}[A_0^{(1)}(\mathbf{z})^c] + \mathbb{P}[A_2^{(1)}(\mathbf{z})^c]. \quad (31)$$

By Lemma 4.9, for ε sufficiently small and n sufficiently large,

$$\begin{aligned} \mathbb{P}[A_2^{(1)}(\mathbf{z})^c] &\leq 2L_0 |\mathcal{Y}|^n \exp \left(-L_1 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge X|YU) + f_1(\delta) + f_2(\delta))}}{2 \ln 2} \right) \\ &\quad + 2L_0 \exp \left(-L_2 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge Y|U) + f_1(\delta) + f_4(\delta))}}{4 \ln 2} \right). \end{aligned} \quad (32)$$

In order to bound $\hat{\mathbb{P}}_{\mathbf{z}}^{(1)}[A_0^{(1)}(\mathbf{z})^c]$, note that the sets $A_2^{(1)}(1, \mathbf{z}), \dots, A_2^{(1)}(L_0, \mathbf{z})$ are independent with respect to \mathbb{P} . Thus under $\hat{\mathbb{P}}_{\mathbf{z}}^{(1)}$, the random variables

$$\tilde{W}_{\mathbf{z}}^{(1)}(l_0) := \frac{1}{L_1 L_2} \sum_{l_1, l_2} W_e^{\otimes n}(\mathbf{z} | X^{l_0 l_1}, Y^{l_0 l_2}) 1_{E_0^{(1)}(U^{l_0}, X^{l_0 l_1}, Y^{l_0 l_2})}(\mathbf{z}) \quad (l_0 \in [L_0])$$

retain their independence and are upper-bounded by

$$(1 + 3\varepsilon) \max_{\mathbf{u} \in T_{U, \delta}^n} \hat{\vartheta}_{\mathbf{u}}^{(1)}(\mathbf{z}).$$

We can further bound this last term as follows: for $\mathbf{u} \in T_{U, \delta}^n$, applying (25) and (26),

$$\begin{aligned} \hat{\vartheta}_{\mathbf{u}}^{(1)}(\mathbf{z}) &= \mathbb{E}[W_e^{\otimes n}(\mathbf{z} | X^{11}, Y^{11}) 1_{E_0^{(1)}(\mathbf{u}, X^{11}, Y^{11})}(\mathbf{z}) | U^1 = \mathbf{u}] \\ &\leq \mathbb{E}[W_e^{\otimes n}(\mathbf{z} | X^{11}, Y^{11}) | U^1 = \mathbf{u}] \\ &\leq \frac{1}{P_1^{\otimes n}(T_{X|U, \delta}^n(\mathbf{u}) | \mathbf{u}) P_2^{\otimes n}(T_{Y|U, \delta}^n(\mathbf{u}) | \mathbf{u})} P_{Z|U}^{\otimes n}(\mathbf{z} | \mathbf{u}) \\ &\leq (1 - 2^{-nc_1 \delta^2})^{-2} 2^{-n(H(Z|U) - f_4(\delta))}. \end{aligned}$$

Observing that $\hat{\mathbb{E}}_{\mathbf{z}}^{(1)}[\tilde{W}_{\mathbf{z}}^{(1)}(1)] \in [(1 \pm 3\varepsilon) \hat{\vartheta}^{(1)}(\mathbf{z})]$ and applying Lemma 4.6 and (28) in the usual way yields

$$\begin{aligned} \hat{\mathbb{P}}_{\mathbf{z}}^{(1)}[A_0^{(1)}(\mathbf{z})^c] &\leq 2 \exp \left(-L_0 \cdot \frac{\varepsilon^2 (1 - 2^{-nc \delta^2})^2 2^{n(H(Z|U) - f_4(\delta))} (1 - 3\varepsilon) \hat{\vartheta}^{(1)}(\mathbf{z})}{2(1 + 3\varepsilon) \ln 2} \right) \\ &\leq 2 \exp \left(-L_0 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge U) + f_4(\delta) + f_6(\delta))}}{4 \ln 2} \right) \end{aligned}$$

if ε is sufficiently small and n sufficiently large. Inserting this and (32) in (31) completes the proof. \square

We finally note that results analogous to Lemma 4.7-4.10 hold where the roles of X and Y are exchanged. We denote the corresponding events by $A_*^{(1)}(l_0, l_2)'$ and $A_1^{(1)}(l_0, l_2, \mathbf{z})', A_2^{(1)}(l_0, \mathbf{z})', A_0^{(1)}(\mathbf{z})'$.

Secrecy for Case 0 and 1: The following lemma links the above probabilistic bounds to secrecy. In the next subsection, roughly speaking, we will associate a family \mathcal{F} to every message triple (k_0, k_1, k_2) . If L_0, L_1, L_2 are large enough, the bounds of Lemma 4.11 are satisfied for every such \mathcal{F} with high probability. Hence there is a joint realization of the \mathcal{F} such that the statement of the lemma is satisfied for every message triple. By an appropriate choice of random code one then obtains (22).

Lemma 4.11. *Denote by $p^{(1)}$ the bound on $\mathbb{P}[A_2^{(1)}(l_0, \mathbf{z})^c]$ derived in Lemma 4.9. Let $\{\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2} : (l_0, l_1, l_2) \in [L_0] \times [L_1] \times [L_2]\}$ be a realization of \mathcal{F} satisfying the conditions of*

$$\bigcap_{l_0, l_2} A_*^{(1)}(l_0, l_2), \quad (33)$$

$$\bigcap_{l_0, l_2} \bigcap_{\mathbf{z} \in \mathcal{Z}^n} A_1^{(1)}(l_0, l_2, \mathbf{z}), \quad (34)$$

$$\bigcap_{l_0} \bigcap_{\mathbf{z} \in \mathcal{Z}^n} A_2^{(1)}(l_0, \mathbf{z}), \quad (35)$$

$$\bigcap_{\mathbf{z} \in F_0^{(1)}} A_0^{(1)}(\mathbf{z}). \quad (36)$$

Then

$$\|\hat{\vartheta}^{(1)} - \frac{1}{L_0 L_1 L_2} \sum_{l_0, l_1, l_2} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2})\| \leq 20\varepsilon + 9 \cdot 2^{-nc\delta^2} + L_0 |\mathcal{Z}|^n p^{(1)}.$$

The same inequality is true if we require conditions (33')-(36') which contain the primed equivalents of (33)-(36) defined at the end of the previous paragraph. If $L_0 = 1$, then (36) and (36') do not have to hold.

We now prove the above lemma. We have

$$\begin{aligned} & \|\hat{\vartheta}^{(1)} - \frac{1}{L_0 L_1 L_2} \sum_{l_0, l_1, l_2} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2})\| \\ & \leq \|\hat{\vartheta}^{(1)} - \frac{1}{L_0 L_1 L_2} \sum_{l_0, l_1, l_2} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2}) 1_{E_0^{(1)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2})} 1_{F_0^{(1)}}\| \end{aligned} \quad (37)$$

$$+ \|\frac{1}{L_0 L_1 L_2} \sum_{l_0, l_1, l_2} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2}) 1_{E_0^{(1)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2})} (1 - 1_{F_0^{(1)}})\| \quad (38)$$

$$+ \|\frac{1}{L_0 L_1 L_2} \sum_{l_0, l_1, l_2} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2}) 1_{E_2^{(1)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2})} (1 - 1_{F_2^{(1)}(\mathbf{u}^{l_0})})\| \quad (39)$$

$$+ \|\frac{1}{L_0 L_1 L_2} \sum_{l_0, l_1, l_2} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2}) 1_{E_1^{(1)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2})} (1 - 1_{F_1^{(1)}(\mathbf{u}^{l_0}, \mathbf{y}^{l_0 l_2})})\| \quad (40)$$

$$+ \|\frac{1}{L_0 L_1 L_2} \sum_{l_0, l_1, l_2} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2}) (1 - 1_{E_1^{(1)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2})})\|. \quad (41)$$

Due to (36), we know that (37) $\leq 5\varepsilon$.

Next we consider (40). Due to (34) we have

$$\begin{aligned} & (40) \\ & \leq 1 - \frac{1}{L_0 L_1 L_2} \sum_{l_0, l_1, l_2} W_e^{\otimes n}(E_2^{(1)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2}) | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2}) \\ & \leq 1 - \frac{1 - \varepsilon}{L_0 L_2} \sum_{l_0, l_2} \hat{\vartheta}_{\mathbf{u}^{l_0} \mathbf{y}^{l_0 l_2}}^{(1)}(\mathcal{X}^n) \end{aligned}$$

(we defined the general measure of a set in the notation section at the beginning of the paper). The support of $\vartheta_{\mathbf{u}^{l_0} \mathbf{y}^{l_0 l_2}}^{(1)}$ is contained in $T_{Z|YU, 2|\mathcal{X}|\delta}^n(\mathbf{y}^{l_0 l_2}, \mathbf{u}^{l_0})$, so by the definition of $F_1^{(1)}(\mathbf{u}^{l_0}, \mathbf{y}^{l_0 l_2})$ we obtain

$$\hat{\vartheta}_{\mathbf{u}^{l_0} \mathbf{y}^{l_0 l_2}}^{(1)}(\mathcal{X}^n) \geq \vartheta_{\mathbf{u}^{l_0} \mathbf{y}^{l_0 l_2}}^{(1)}(\mathcal{X}^n) - \varepsilon. \quad (42)$$

Lemma 4.12. *If $\mathbf{u} \in T_{U, \delta}^n$ and $\mathbf{y} \in T_{Y|U, \delta}^n(\mathbf{u})$, then*

$$\vartheta_{\mathbf{u} \mathbf{y}}^{(1)}(\mathcal{X}^n) \geq 1 - 2 \cdot 2^{-nc\delta^2}.$$

Proof. First of all note that

$$\begin{aligned} & \vartheta_{\mathbf{u} \mathbf{y}}^{(1)}(\mathcal{X}^n) \\ & = \mathbb{E}[W_e^{\otimes n}(E_1^{(1)}(\mathbf{u}, X^{11}, \mathbf{y}) | X^{11}, \mathbf{y}) | U^1 = \mathbf{u}] \\ & \geq \mathbb{E}[W_e^{\otimes n}(E_1^{(1)}(\mathbf{u}, X^{11}, \mathbf{y}) | X^{11}, \mathbf{y}); X^{11} \in T_{X|YU, \delta}^n(\mathbf{y}, \mathbf{u}) | U^1 = \mathbf{u}]. \end{aligned} \quad (43)$$

Now we claim that for $\mathbf{x} \in T_{X|YU,\delta}^n(\mathbf{y}, \mathbf{u})$

$$T_{Z|YXU,\delta}^n(\mathbf{y}, \mathbf{x}, \mathbf{u}) \subset T_{Z|YU,2|\mathcal{X}|\delta}^n(\mathbf{y}, \mathbf{u}). \quad (44)$$

To verify this, let $(z, y, u) \in \mathcal{Z} \times \mathcal{Y} \times \mathcal{U}$ and $\mathbf{z} \in T_{Z|YXU,\delta}^n(\mathbf{y}, \mathbf{x}, \mathbf{u})$. Then

$$\begin{aligned} & \left| \frac{1}{n} N(z, y, u | \mathbf{z}, \mathbf{y}, \mathbf{u}) - P_{Z|YU}(z | y, u) \frac{1}{n} N(y, u | \mathbf{y}, \mathbf{u}) \right| \\ & \leq \sum_x \left| \frac{1}{n} N(z, y, x, u | \mathbf{z}, \mathbf{y}, \mathbf{x}, \mathbf{u}) - W(z | x, y) \frac{1}{n} N(y, x, u | \mathbf{y}, \mathbf{x}, \mathbf{u}) \right| \\ & \quad + \sum_x W(z | x, y) \left| \frac{1}{n} N(y, x, u | \mathbf{y}, \mathbf{x}, \mathbf{u}) - P_{X|YU}(x | y, u) \frac{1}{n} N(y, u | \mathbf{y}, \mathbf{u}) \right| \\ & \leq 2|\mathcal{X}|\delta. \end{aligned}$$

This proves (44). Due to the choice of $f_2(\delta)$ and to (26), we thus see that $T_{Z|YXU,\delta}^n(\mathbf{y}, \mathbf{x}, \mathbf{u})$ is contained in $E_1^{(1)}(\mathbf{u}, \mathbf{x}, \mathbf{y})$ for $\mathbf{x} \in T_{X|YU,\delta}^n(\mathbf{y}, \mathbf{u})$, and we have that (43) is lower-bounded by

$$\mathbb{E}[W_e^{\otimes n}(T_{Z|YXU,\delta}^n(\mathbf{y}, X^{11}, \mathbf{u}) | X^{11}, \mathbf{y}); X^{11} \in T_{X|YU,\delta}^n(\mathbf{y}, \mathbf{u}) | U^1 = \mathbf{u}]. \quad (45)$$

Further, as in the proof of Lemma 4.7 one sees that

$$\mathbb{P}[X^{11} \in T_{X|YU,\delta}^n(\mathbf{y}, \mathbf{u}) | U^1 = \mathbf{u}] \geq 1 - \frac{2^{-nc\delta^2}}{1 - 2^{-nc\delta^2}}. \quad (46)$$

Due to (46) and (25), we can lower-bound (45) for sufficiently large n by

$$(1 - 2^{-nc\delta^2}) \cdot \left(1 - \frac{2^{-nc\delta^2}}{1 - 2^{-nc\delta^2}} \right) \geq 1 - 2 \cdot 2^{-nc\delta^2},$$

which proves Lemma 4.12. \square

Using (42) and Lemma 4.12 we can conclude that

$$(40) \leq 2(\varepsilon + 2^{-nc\delta^2}).$$

One starts similarly for (39). We have by (35)

$$\begin{aligned} (39) & \leq 1 - \frac{1}{L_0 L_1 L_2} \sum_{l_0, l_1, l_2} W_e^{\otimes n}(E_0^{(1)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2}) | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2}) \\ & \leq 1 - \frac{(1 - 3\varepsilon)}{L_0} \sum_{l_0} \hat{\vartheta}_{\mathbf{u}^{l_0}}^{(1)}(\mathcal{Z}^n). \end{aligned}$$

As the support of $\vartheta_{\mathbf{u}^{l_0}}^{(1)}$ is contained in $T_{Z|U,3|\mathcal{Y}||\mathcal{X}|\delta}^n(\mathbf{u}^{l_0})$, we can lower-bound $\hat{\vartheta}_{\mathbf{u}^{l_0}}^{(1)}(\mathcal{Z}^n)$ by $\vartheta_{\mathbf{u}^{l_0}}^{(1)}(\mathcal{Z}^n) - \varepsilon$. Using (42) and Lemma 4.12, we have

$$\vartheta_{\mathbf{u}^{l_0}}^{(1)}(\mathcal{Z}^n) = \mathbb{E}[\hat{\vartheta}_{\mathbf{u}^{l_0} Y^{11}}^{(1)}(\mathcal{Z}^n) | U^1 = \mathbf{u}^{l_0}] \geq 1 - 2 \cdot 2^{-nc\delta^2} - \varepsilon, \quad (47)$$

so we conclude

$$(39) \leq 5\varepsilon + 2 \cdot 2^{-nc\delta^2}.$$

For (38), one has by (36)

$$\begin{aligned} (38) &\leq 1 - \frac{1}{L_0 L_1 L_2} \sum_{l_0, l_1, l_2} W_e^{\otimes n}(E_0^{(1)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2}) \cap F_0^{(1)} | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2}) \\ &\leq 1 - (1 - 5\varepsilon) \hat{\vartheta}^{(1)}(F_0^{(1)}). \end{aligned}$$

It remains to lower-bound $\hat{\vartheta}^{(1)}(F_0^{(1)})$. Observe that the support of $\vartheta^{(1)}$ is restricted to $T_{Z, 4|\mathcal{Y}||\mathcal{X}||\mathcal{U}|\delta}^n$, so due to the definition of $F_0^{(1)}$, one has $\hat{\vartheta}^{(1)}(F_0^{(1)}) = \vartheta^{(1)}(F_0^{(1)}) \geq \vartheta^{(1)}(\mathcal{Z}^n) - \varepsilon$. Further,

$$\begin{aligned} \vartheta^{(1)}(\mathcal{Z}^n) &= \sum_{\mathbf{z} \in \mathcal{Z}^n} \hat{\mathbb{E}}_{\mathbf{z}}^{(1)}[\hat{\theta}_{U^1}^{(1)}(\mathbf{z})] \\ &\geq \mathbb{E}[\theta_{U^1}^{(1)}(\mathcal{Z}^n)] - \sum_{\mathbf{z} \in \mathcal{Z}^n} \mathbb{P}[A_2^{(1)}(\mathbf{z})^c] \\ &= \mathbb{E}[\theta_{U^1}^{(1)}(\mathcal{Z}^n)] - L_0 |\mathcal{Z}|^n p^{(1)}. \end{aligned}$$

In (47), the integrand of $\mathbb{E}[\theta_{U^1}^{(1)}(\mathcal{Z}^n)]$ was lower-bounded by $1 - 2 \cdot 2^{-nc\delta^2} - \varepsilon$. We conclude

$$(38) \leq 7\varepsilon + 2 \cdot 2^{-nc\delta^2} + L_0 |\mathcal{Z}|^n p^{(1)}.$$

Finally, we use condition (33) to bound (41). We have

$$\begin{aligned} (41) &= \frac{1}{L_0 L_1 L_2} \sum_{l_0, l_1, l_2} W_e^{\otimes n}(E_1^{(1)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2})^c | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2}) \\ &= \frac{1}{L_0 L_2} \sum_{l_0, l_2} \left(\frac{1}{L_1} \sum_{l_1: \mathbf{x}^{l_0 l_1} \in T_{X|YU, \delta}^n(\mathbf{y}^{l_0 l_2}, \mathbf{u}^{l_0})} W_e^{\otimes n}(E_1^{(1)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2})^c | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2}) \right. \\ &\quad \left. + \frac{1}{L_1} \sum_{l_1: \mathbf{x}^{l_0 l_1} \notin T_{X|YU, \delta}^n(\mathbf{y}^{l_0 l_2}, \mathbf{u}^{l_0})} W_e^{\otimes n}(E_1^{(1)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2})^c | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0 l_2}) \right). \end{aligned} \quad (49)$$

For every (l_0, l_2) , we use $T_{Z|YXU, \delta}^n(\mathbf{y}, \mathbf{x}, \mathbf{u}) \subset E_1^{(1)}(\mathbf{u}, \mathbf{x}, \mathbf{y})$ for $(\mathbf{u}, \mathbf{x}, \mathbf{y}) \in T_{U, \delta}^n \times T_{Y|U, \delta}^n(\mathbf{u}) \times T_{X|YU, \delta}^n(\mathbf{y}, \mathbf{u})$ as shown in the proof of Lemma 4.12 to upper-bound the term in (49) by $2^{-nc\delta^2}$. For (50), we know from assumption (33) that it is at most $1 - (1 - \varepsilon)(1 - 2 \cdot 2^{-nc\delta^2})$. Thus

$$(41) \leq 2^{-nc\delta^2} + (1 - \varepsilon)(1 - 2 \cdot 2^{-nc\delta^2}) \leq \varepsilon + 3 \cdot 2^{-nc\delta^2}.$$

Collecting the bounds on (37)-(41), we obtain a total upper bound of

$$20eps + 9 \cdot 2^{-nc\delta^2} + L_0 |\mathcal{Z}|^n p^{(1)}.$$

This finishes the proof of Lemma 4.11.

Bounds for Case 2: Now we specialize to the case that $L_2 = 1$, but L_0 and L_1 arbitrary. This reduces the number of Chernoff-type estimates needed by one. Lemma 4.8 carries over, Lemma 4.9 is not needed, but Lemma 4.10 changes. We write $Y^{l_0 1} =: Y^{l_0}$. The definitions of $E_1^{(1)}(\mathbf{u}, \mathbf{x}, \mathbf{y})$, $F_1^{(1)}(\mathbf{u}, \mathbf{y})$ and $\vartheta_{\mathbf{u}\mathbf{y}}^{(1)}$ carry over to this case, we just call them $E_1^{(2)}(\mathbf{u}, \mathbf{x}, \mathbf{y})$, $F_1^{(2)}(\mathbf{u}, \mathbf{y})$ and $\vartheta_{\mathbf{u}\mathbf{y}}^{(2)}$. Further we define

$$E_0^{(2)}(\mathbf{u}, \mathbf{x}, \mathbf{y}) := E_1^{(2)}(\mathbf{u}, \mathbf{x}, \mathbf{y}) \cap F_1^{(2)}(\mathbf{u}, \mathbf{y}).$$

For every l_0 , let $A_1^{(2)}(l_0, \mathbf{z}) := A_1^{(1)}(l_0, 1, \mathbf{z})$ and we set $A_1^{(2)}(\mathbf{z}) := A_1^{(2)}(1, \mathbf{z}) \cap \dots \cap A_1^{(2)}(L_0, \mathbf{z})$. We define for every \mathbf{z} a new probability measure by $\hat{\mathbb{P}}_{\mathbf{z}}^{(2)} := \mathbb{P}[\cdot | A_1^{(2)}(\mathbf{z})]$. Let

$$\vartheta^{(2)}(\mathbf{z}) := \hat{\mathbb{E}}_{\mathbf{z}}^{(2)}[\hat{\vartheta}_{U^1 Y^1}^{(2)}(\mathbf{z})].$$

Further let

$$F_0^{(2)} := \{\mathbf{z} \in T_{Z, 4|\mathcal{Y}||\mathcal{X}||\mathcal{U}|\delta}^n : \vartheta^{(2)}(\mathbf{z}) \geq \varepsilon |T_{Z, \delta}^n|^{-1}\}$$

and

$$\hat{\vartheta}^{(2)} = \vartheta^{(2)} \cdot 1_{F_0^{(2)}}.$$

Lemma 4.13. *Let $\mathbf{z} \in F_0^{(2)}$. Let $A_0^{(2)}(\mathbf{z})$ be the event*

$$\frac{1}{L_0 L_1} \sum_{l_0, l_1} W_e^{\otimes n}(\mathbf{z} | X^{l_0 l_1}, Y^{l_0}) 1_{E_0^{(2)}(U^{l_0}, X^{l_0 l_1}, Y^{l_0})}(\mathbf{z}) \in [(1 \pm 3\varepsilon) \hat{\vartheta}^{(2)}(\mathbf{z})].$$

Then for ε sufficiently small and n sufficiently large,

$$\begin{aligned} \mathbb{P}[A_0^{(2)}(\mathbf{z})^c] &\leq 2L_0 \exp\left(-L_1 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge X | YU) + f_1(\delta) + f_2(\delta))}}{2 \ln 2}\right) \\ &\quad + 2 \exp\left(-L_0 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge YU) + f_1(\delta) + f_6(\delta))}}{4 \ln 2}\right). \end{aligned}$$

Proof. We have

$$\mathbb{P}[A_0^{(2)}(\mathbf{z})^c] \leq \hat{\mathbb{P}}_{\mathbf{z}}^{(2)}[A_0^{(2)}(\mathbf{z})^c] + \mathbb{P}[A_1^{(2)}(\mathbf{z})^c]. \quad (51)$$

By Lemma 4.8, we know that

$$\mathbb{P}[A_1^{(2)}(\mathbf{z})^c] \leq 2L_0 \exp\left(-L_1 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge X | YU) + f_1(\delta) + f_2(\delta))}}{2 \ln 2}\right). \quad (52)$$

In order to bound $\mathbb{P}_{\mathbf{z}}^{(2)}[A_0^{(2)}(\mathbf{z})]$, note that the sets $A_1^{(2)}(1, \mathbf{z}), \dots, A_1^{(2)}(L_0, \mathbf{z})$ are independent with respect to \mathbb{P} . Thus under $\hat{\mathbb{P}}_{\mathbf{z}}^{(2)}$, the random variables

$$\tilde{W}_{\mathbf{z}}^{(2)}(l_0) := \frac{1}{L_1} \sum_{l_1} W_e^{\otimes n}(\mathbf{z}|X^{l_0 l_1}, Y^{l_0}) 1_{E_0^{(2)}(U^{l_0}, X^{l_0 l_1}, Y^{l_0})}(\mathbf{z}) \quad (l_0 \in [L_0])$$

retain their independence and are upper-bounded by

$$(1 + \varepsilon) \max_{\mathbf{u} \in T_{U, \delta}^n} \max_{\mathbf{y} \in T_{Y|U, \delta}^n(\mathbf{u})} \hat{\vartheta}_{\mathbf{u}\mathbf{y}}^{(2)}(\mathbf{z}).$$

We can further bound this last term as follows: for $\mathbf{u} \in T_{U, \delta}^n$ and $\mathbf{y} \in T_{Y|U, \delta}^n(\mathbf{u})$ one obtains by (25) and (26)

$$\begin{aligned} \hat{\vartheta}_{\mathbf{u}\mathbf{y}}^{(2)}(\mathbf{z}) &\leq \mathbb{E}[W_e^{\otimes n}(\mathbf{z}|X^{11}, \mathbf{y})|U^{l_0} = \mathbf{u}] \\ &\leq \frac{1}{1 - 2^{-nc\delta^2}} P_{Z|YU}^{\otimes n}(\mathbf{z}|\mathbf{y}, \mathbf{u}) \\ &\leq \frac{1}{1 - 2^{-nc\delta^2}} 2^{-n(H(Z|YU) - f_1(\delta))}. \end{aligned}$$

Observing that $\hat{\mathbb{E}}_{\mathbf{z}}[\tilde{W}_{\mathbf{z}}^{(2)}(1)] \in [(1 \pm \varepsilon)\hat{\vartheta}^{(2)}(\mathbf{z})]$ and applying Lemma 4.6 in the usual way yields

$$\begin{aligned} \hat{\mathbb{P}}_{\mathbf{z}}[A_0^{(2)}(\mathbf{z})] &\leq 2 \exp \left(-L_0 \cdot \frac{\varepsilon^2 (1 - 2^{-nc\delta^2}) 2^{n(H(Z|YU) - f_1(\delta))} (1 - \varepsilon) \hat{\vartheta}^{(2)}(\mathbf{z})}{2(1 + \varepsilon) \ln 2} \right) \\ &\leq 2 \exp \left(-L_0 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge YU) + f_1(\delta) + f_6(\delta))}}{4 \ln 2} \right) \end{aligned}$$

if ε is sufficiently small and n sufficiently large. Inserting this and (52) in (51) completes the proof. \square

Again we note that a result analogous to Lemma 4.13 holds where the roles of X and Y are exchanged. Setting $A_*^{(2)}(l_0) := A_*^{(1)}(l_0, 1)$, we denote the events corresponding to such an exchange by $A_*^{(2)}(l_0)'$ and $A_1^{(2)}(l_0, \mathbf{z})', A_0^{(2)}(\mathbf{z})'$.

Secrecy for Case 2:

Lemma 4.14. *Denote by $p^{(2)}$ the bound on $\mathbb{P}[A_1^{(2)}(l_0, \mathbf{z})^c]$ derived in Lemma 4.8. Let $\{\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0} : (l_0, l_1, l_2) \in [L_0] \times [L_1] \times [L_2]\}$ be a realization of \mathcal{F} satisfying the conditions of*

$$\bigcap_{l_0} A_*^{(2)}(l_0), \quad (53)$$

$$\bigcap_{l_0} \bigcap_{\mathbf{z} \in \mathcal{Z}^n} A_1^{(2)}(l_0, \mathbf{z}), \quad (54)$$

$$\bigcap_{\mathbf{z} \in F_0^{(2)}} A_0^{(2)}(\mathbf{z}). \quad (55)$$

Then

$$\|\hat{\vartheta}^{(2)} - \frac{1}{L_0 L_1} \sum_{l_0, l_1} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0})\| \leq 9\varepsilon + 7 \cdot 2^{-nc\delta^2} + L_0 |\mathcal{X}|^n p^{(2)}.$$

The same inequality is true if we require conditions (53')-(55') which contain the primed equivalents of (53)-(55) defined at the end of the previous paragraph.

We use this subsection to prove the above lemma. We have

$$\begin{aligned} & \|\hat{\vartheta}^{(2)} - \frac{1}{L_0 L_1} \sum_{l_0, l_1} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0})\| \\ & \leq \|\hat{\vartheta}^{(2)} - \frac{1}{L_0 L_1} \sum_{l_0, l_1} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0}) 1_{E_0^{(2)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0})} 1_{F_0^{(2)}}\| \end{aligned} \quad (56)$$

$$+ \left\| \frac{1}{L_0 L_1} \sum_{l_0, l_1} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0}) 1_{E_0^{(2)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0})} (1 - 1_{F_0^{(2)}}) \right\| \quad (57)$$

$$+ \left\| \frac{1}{L_0 L_1} \sum_{l_0, l_1} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0}) 1_{E_1^{(2)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0})} (1 - 1_{F_1^{(2)}(\mathbf{u}^{l_0}, \mathbf{y}^{l_0})}) \right\| \quad (58)$$

$$+ \left\| \frac{1}{L_0 L_1} \sum_{l_0, l_1} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0}) (1 - 1_{E_1^{(2)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0})}) \right\|. \quad (59)$$

Due to (55), we know that (56) $\leq \varepsilon$.

Next we consider (58). Due to (54), we have

$$\begin{aligned} (58) & \leq 1 - \frac{1}{L_0 L_1} \sum_{l_0, l_1} W_e^{\otimes n}(E_0^{(2)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0}) | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0}) \\ & \leq 1 - \frac{1 - \varepsilon}{L_0} \sum_{l_0} \hat{\vartheta}_{\mathbf{u}^{l_0} \mathbf{y}^{l_0}}^{(2)}(\mathcal{X}^n). \end{aligned}$$

As for Case 3, one lower-bounds $\hat{\vartheta}_{\mathbf{u}^{l_0} \mathbf{y}^{l_0}}^{(2)}(\mathcal{X}^n) \geq \vartheta_{\mathbf{u}^{l_0} \mathbf{y}^{l_0}}^{(2)}(\mathcal{X}^n) - \varepsilon$ by $1 - 2 \cdot 2^{-nc\delta^2} - \varepsilon$. Thus we can conclude that

$$(58) \leq 2(\varepsilon + 2^{-nc\delta^2}).$$

For (57), we have by (54)

$$\begin{aligned} (57) & \leq 1 - \frac{1}{L_0 L_1} \sum_{l_0, l_1} W_e^{\otimes n}(E_0^{(2)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0}) \cap F_0^{(2)} | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0}) \\ & \leq 1 - (1 - 3\varepsilon) \hat{\vartheta}^{(2)}(F_0^{(2)}). \end{aligned}$$

It remains to lower-bound $\hat{\vartheta}^{(2)}(F_0^{(2)}) \geq \vartheta^{(2)}(\mathcal{X}^n) - \varepsilon$. As in the lower bound on $\theta^{(1)}(\mathcal{X}^n)$ above, one obtains the bound

$$\vartheta^{(2)}(\mathcal{X}^n) \geq 1 - 2 \cdot 2^{-nc\delta^2} - \varepsilon.$$

Thus we conclude

$$(57) \leq 5\varepsilon + 2 \cdot 2^{-nc\delta^2}.$$

Finally, we use condition (53) to bound (59). We have

$$\begin{aligned} (59) &= \frac{1}{L_0 L_1} \sum_{l_0, l_1} W_e^{\otimes n}(E_1^{(2)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0}) | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0}) \\ &= \frac{1}{L_0} \sum_{l_0} \left(\frac{1}{L_1} \sum_{l_1: \mathbf{x}^{l_0 l_1} \in T_{X|YU, \delta}^n(\mathbf{y}^{l_0}, \mathbf{u}^{l_0})} W_e^{\otimes n}(E_1^{(2)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0}) | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0}) \right) \quad (60) \\ &\quad + \frac{1}{L_1} \sum_{l_1: \mathbf{x}^{l_0 l_1} \notin T_{X|YU, \delta}^n(\mathbf{y}^{l_0}, \mathbf{u}^{l_0})} W_e^{\otimes n}(E_1^{(2)}(\mathbf{u}^{l_0}, \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0}) | \mathbf{x}^{l_0 l_1}, \mathbf{y}^{l_0}) \quad (61) \end{aligned}$$

For every l_0 , the summand appearing in (60) can be upper-bounded by $2^{-nc\delta^2}$. By assumption (53), (61) is upper-bounded by $1 - (1 - \varepsilon)(1 - 2 \cdot 2^{-nc\delta^2})$. Thus

$$(59) \leq \varepsilon + 3 \cdot 2^{-nc\delta^2}.$$

Collecting the bounds for (56)-(59), we obtain a total upper bound of

$$9\varepsilon + 7 \cdot 2^{-nc\delta^2} + L_0 |\mathcal{X}|^n p^{(2)}.$$

This finishes the proof of Lemma 4.14.

Bounds for Case 3: Now we treat the case $L_1 = L_2 = 1$. Lemma 4.15 is the analog of Lemma 4.7, the proofs are analogous.

Lemma 4.15. *Let the event $A_*^{(3)}$ be defined by*

$$A_*^{(3)} := \{ | \{ l_0 \in [L_0] : X^{l_0} \in T_{X|YU, \delta}^n(Y^{l_0}, U^{l_0}) \} | \geq (1 - \varepsilon)(1 - 2 \cdot 2^{-nc_1\delta^2}) L_0 \}.$$

Then

$$\mathbb{P}[(A_*^{(3)})^c] \leq \exp \left(-L_0 \cdot \frac{\varepsilon^2(1 - 2 \cdot 2^{-nc_1\delta^2})}{2 \ln 2} \right).$$

Let

$$E^{(3)}(\mathbf{x}, \mathbf{y}) := \{ \mathbf{z} \in T_{Z, 4|\mathcal{X}||\mathcal{Y}||\mathcal{Z}|, \delta}^n : W_e^{\otimes n}(\mathbf{z} | \mathbf{x}, \mathbf{y}) \leq 2^{-n(H(Z|XY) - f_2(\delta))} \},$$

where $f_2(\delta) = \tau(P_{XYZ}, 3\delta, \delta)$. Let

$$\vartheta^{(3)}(\mathbf{z}) := \mathbb{E}[W_e^{\otimes n}(\mathbf{z} | X^1, Y^1) 1_{E_1(X^1, Y^1)}(\mathbf{z})]$$

and for

$$F^{(3)} := \{ \mathbf{z} \in T_{Z, 4|\mathcal{X}||\mathcal{Y}||\mathcal{Z}|, \delta}^n : \vartheta(\mathbf{z}) \geq \varepsilon |T_{Z, \delta}^n|^{-1} \}$$

define the measure

$$\hat{\vartheta}^{(3)} := \vartheta^{(3)} \cdot 1_{F^{(3)}}.$$

Lemma 4.16. *Let $\mathbf{z} \in F^{(3)}$. Let $A^{(3)}(\mathbf{z})$ be the event that*

$$\frac{1}{L_0} \sum_{l_0} W_e^{\otimes n}(\mathbf{z} | X^{l_0}, Y^{l_0}) 1_{E^{(3)}(X^{l_0}, Y^{l_0})}(\mathbf{z}) \in [(1 \pm \varepsilon) \hat{\vartheta}^{(3)}(\mathbf{z})].$$

Then for $f_1(\delta) = \tau(P_{UYZ}, 4|\mathcal{X}||\mathcal{Y}|\delta, \delta)$,

$$\mathbb{P}[A^{(3)}(\mathbf{z})^c] \leq 2 \exp \left(-L_0 \cdot \frac{\varepsilon^3 2^{-n(I(Z \wedge XY) + f_1(\delta) + f_2(\delta))}}{2 \ln 2} \right).$$

The proof of this lemma is analogous to that of Lemma 4.8.

Secrecy for Case 3:

Lemma 4.17. *Let $\{(\mathbf{u}^{l_0}, \mathbf{x}^{l_0}, \mathbf{y}^{l_0})\}$ be a realization of \mathcal{F} satisfying the conditions of*

$$A_*^{(3)}, \tag{62}$$

$$\bigcap_{\mathbf{z} \in F^{(3)}} A^{(3)}(\mathbf{z}). \tag{63}$$

Then for sufficiently large n ,

$$\|\hat{\vartheta}^{(3)} - \frac{1}{L_0} \sum_{l_0} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0}, \mathbf{y}^{l_0})\| \leq 4\varepsilon + 5 \cdot 2^{-nc\delta^2}. \tag{64}$$

We use this subsection to prove the above lemma. We have

$$\begin{aligned} & \|\hat{\vartheta}^{(3)} - \frac{1}{L_0} \sum_{l_0} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0}, \mathbf{y}^{l_0})\| \\ & \leq \|\hat{\vartheta}^{(3)} - \frac{1}{L_0} \sum_{l_0} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0}, \mathbf{y}^{l_0}) 1_{E^{(3)}(\mathbf{x}^{l_0}, \mathbf{y}^{l_0})} 1_{F^{(3)}}\| \end{aligned} \tag{65}$$

$$+ \left\| \frac{1}{L_0} \sum_{l_0} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0}, \mathbf{y}^{l_0}) 1_{E^{(3)}(\mathbf{x}^{l_0}, \mathbf{y}^{l_0})} (1 - 1_{F^{(3)}}) \right\| \tag{66}$$

$$+ \left\| \frac{1}{L_0} \sum_{l_0} W_e^{\otimes n}(\cdot | \mathbf{x}^{l_0}, \mathbf{y}^{l_0}) (1 - 1_{E^{(3)}(\mathbf{x}^{l_0}, \mathbf{y}^{l_0})}) \right\|. \tag{67}$$

Due to (63) we have (65) $\leq \varepsilon$.

Next we bound (66). Again using (63),

$$\begin{aligned} (66) & \leq 1 - \frac{1}{L_0} \sum_{l_0} W_e^{\otimes n}(E^{(3)}(\mathbf{x}^{l_0}, \mathbf{y}^{l_0}) \cap F^{(3)} | \mathbf{x}^{l_0}, \mathbf{y}^{l_0}) \\ & \leq 1 - (1 - \varepsilon) \hat{\vartheta}^{(3)}(F^{(3)}). \end{aligned} \tag{68}$$

As in Case 1 and 2, $\hat{\vartheta}^{(3)}(F^{(3)})$ can be lower-bounded by $1 - 2 \cdot 2^{-nc\delta^2} - \varepsilon$, so

$$(66) \leq 1 - (1 - \varepsilon)(1 - 2 \cdot 2^{-nc\delta^2} - \varepsilon) \leq 2(\varepsilon + 2^{-nc\delta^2}).$$

Finally, the third term (67) equals

$$\begin{aligned} & \frac{1}{L_0} \sum_{l_0} W_e^{\otimes n}(E^{(3)}(\mathbf{x}^{l_0}, \mathbf{y}^{l_0})^c | \mathbf{x}^{l_0}, \mathbf{y}^{l_0}) \\ &= \frac{1}{L_0} \sum_{l_0: \mathbf{x}^{l_0} \in T_{X|YU, \delta}(\mathbf{y}^{l_0}, \mathbf{u}^{l_0})} W_e^{\otimes n}(E^{(3)}(\mathbf{x}^{l_0}, \mathbf{y}^{l_0})^c | \mathbf{x}^{l_0}, \mathbf{y}^{l_0}) \end{aligned} \quad (69)$$

$$+ \frac{1}{L_0} \sum_{l_0: \mathbf{x}^{l_0} \notin T_{X|YU, \delta}(\mathbf{y}^{l_0}, \mathbf{u}^{l_0})} W_e^{\otimes n}(E^{(3)}(\mathbf{x}^{l_0}, \mathbf{y}^{l_0})^c | \mathbf{x}^{l_0}, \mathbf{y}^{l_0}). \quad (70)$$

and is lower-bounded by

$$(67) \leq 2^{-nc\delta^2} + (1 - \varepsilon)(1 - 2 \cdot 2^{-nc\delta^2}) \leq \varepsilon + 3 \cdot 2^{-nc\delta^2}.$$

Combining the above bounds, we can conclude that

$$(65) + (66) + (67) \leq 4\varepsilon + 5 \cdot 2^{-nc\delta^2},$$

which completes the proof of Lemma 4.17.

4.4 Random Coding for the Non-Wiretap MAC with Common Message

Assume we are given another family of random variables

$$\mathcal{F}' := \bigcup_{l_0 \in [L_0]} (U^{l'_0}, \mathcal{F}'_{l'_0})$$

with $\mathcal{F}'_{l'_0} = \{X^{l'_0 l'_1}, Y^{l'_0 l'_2} : l'_1, l'_2 \in [L'_1] \times [L'_2]\}$ for other positive integers L'_0, L'_1, L'_2 with blocklength n' which is independent of \mathcal{F} , but which has the same structure as \mathcal{F} and whose distribution is defined according to the same p as \mathcal{F} . Define the rate set $\tilde{\mathcal{R}}(p)$ by the bounds

$$\begin{aligned} \tilde{R}_1 &\leq I(T \wedge X | YU), \\ \tilde{R}_2 &\leq I(T \wedge Y | XU), \\ \tilde{R}_1 + \tilde{R}_2 &\leq I(T \wedge XY | U), \\ \tilde{R}_0 + \tilde{R}_1 + \tilde{R}_2 &\leq I(T \wedge XY). \end{aligned}$$

Assume that for some $0 < \eta < I_* := \min\{I_\nu > 0 : \nu = 1, 2, 3, 4\}$ we have

$$\begin{aligned}\frac{n \log L_1 + n' \log L'_1}{n + n'} &\leq [I(T \wedge X|YU) - \eta]_+, \\ \frac{n \log L_2 + n' \log L'_2}{n + n'} &\leq [I(T \wedge Y|XU) - \eta]_+, \\ \frac{n \log(L_1 L_2) + n' \log(L'_1 L'_2)}{n + n'} &\leq [I(T \wedge XY|U) - \eta]_+, \\ \frac{n \log(L_0 L_1 L_2) + n' \log(L'_0 L'_1 L'_2)}{n + n'} &\leq [I(T \wedge XY) - \eta]_+.\end{aligned}$$

Define a new family of random vectors

$$\mathcal{F} \circ \mathcal{F}' := \{\tilde{U}^{l_0 l'_0}, \tilde{X}^{l_0 l'_0 l_1 l'_1}, \tilde{Y}^{l_0 l'_0 l_2 l'_2}\}$$

by concatenating the corresponding elements of \mathcal{F} and \mathcal{F}' , so e.g. $\tilde{U}^{l_0 l'_0} = (U^{l_0}, U^{l'_0}) \in \mathcal{U}^{n+n'}$, $\tilde{X}^{l_0 l'_0 l_1 l'_1} = (X^{l_0 l_1}, X^{l'_0 l'_1}) \in \mathcal{X}^{n+n'}$.

Lemma 4.18. *For any $\delta, \eta > 0$ there are $\zeta_1, \zeta_2 = \zeta_1(\eta, \delta), \zeta_2(\eta, \delta) > 0$ such that the probability of the event A_{MAC} that the family*

$$\{\tilde{X}^{l_0 l'_0 l_1 l'_1}, \tilde{Y}^{l_0 l'_0 l_2 l'_2} : (l_0, l'_0, l_1, l'_1, l_2, l'_2)\}$$

is the codeword set of a deterministic MAC code with average error at most $\exp(-(n+n')\zeta_1)$ is lower-bounded by $1 - \exp(-(n+n')\zeta_2)$. The same result is true if it is formulated only for \mathcal{F} or \mathcal{F}' without concatenation.

Proof. The difference to standard random coding proofs is that the random variables from \mathcal{F} and \mathcal{F}' are conditioned on typicality. Using the random sets

$$E^{l_0 l'_0 l_1 l'_1 l_2 l'_2} := \{\mathbf{t} \in \mathcal{T}^n : (\tilde{U}^{l_0 l'_0}, \tilde{X}^{l_0 l'_0 l_1 l'_1}, \tilde{Y}^{l_0 l'_0 l_2 l'_2}, \mathbf{t}) \in T_{UXYT, \delta}^n\},$$

we define the decoding sets $F^{l_0 l'_0 l_1 l'_1 l_2 l'_2}$ by deciding for $(l_0, l'_0, l_1, l'_1, l_2, l'_2)$ if the output is contained in $E^{l_0 l'_0 l_1 l'_1 l_2 l'_2}$ and if at the same time it is not contained in any $E^{\tilde{l}_0 \tilde{l}'_0 \tilde{l}_1 \tilde{l}'_1 \tilde{l}_2 \tilde{l}'_2}$ for a different message tuple $(\tilde{l}_0, \tilde{l}'_0, \tilde{l}_1, \tilde{l}'_1, \tilde{l}_2, \tilde{l}'_2)$. This decoder is known to be the right decoder in the case where the codewords have the standard i.i.d. structure, i.e. for a family of random variables

$$\{\hat{U}^{l_0 l'_0}, \hat{X}^{l_0 l'_0 l_1 l'_1}, \hat{Y}^{l_0 l'_0 l_2 l'_2}\}$$

where $\hat{U}^{l_0 l'_0} \sim P_U^{\otimes(n+n')}$ and where conditional on $\hat{U}^{l_0 l'_0}$, the $\hat{X}^{l_0 l'_0 l_1 l'_1}$ and $\hat{Y}^{l_0 l'_0 l_2 l'_2}$ are independent with $\hat{X}^{l_0 l'_0 l_1 l'_1} \sim P_{X|U}^{\otimes(n+n')}$ and $\hat{Y}^{l_0 l'_0 l_2 l'_2} \sim P_{Y|U}^{\otimes(n+n')}$. It is easily seen that

$$\begin{aligned}\mathbb{E}[W^{\otimes n}((F^{l_0 l'_0 l_1 l'_1 l_2 l'_2})^c | \tilde{X}^{l_0 l'_0 l_1 l'_1}, \tilde{Y}^{l_0 l'_0 l_2 l'_2})] \\ \leq (1 - 2^{-nc\delta^2})^3 (1 - 2^{-n'c\delta^2})^3 \mathbb{E}[W^{\otimes n}((F^{l_0 l'_0 l_1 l'_1 l_2 l'_2})^c | \hat{X}^{l_0 l'_0 l_1 l'_1}, \hat{Y}^{l_0 l'_0 l_2 l'_2})].\end{aligned}$$

Then the standard random coding proof technique yields the result. The specialization for the case that only \mathcal{F} or \mathcal{F}' is treated is obvious. \square

4.5 Coding

In this subsection we show the achievability of the rate sets $\mathcal{R}^{(\nu)}(p)$ for $\nu = 0, 1, 2, 3$ and appropriate p . For the cases where we showed that $\mathcal{R}^{(\nu)}(p)$ can be written as the union over certain α of rate sets $\mathcal{R}_\alpha^{(\nu)}(p)$, we show the achievability of the latter for every α .

Throughout this section fix a common randomness bound $H_C \geq 0$. Let $\delta > 0$ which will be specified later and n a blocklength which will have to be large enough. Every p considered in this section has the form $p = P_U \otimes (P_{X|U} \otimes P_{Y|U}) \otimes W$. Without loss of generality we may assume that $I(Z \wedge XY) < I(T \wedge XY)$, in particular, $I(T \wedge XY) > 0$. Letting

$$K_0, K_1, K_2, L_0, L_1, L_2, n, \quad K'_0, K'_1, K'_2, L'_0, L'_1, L'_2, n' \quad (71)$$

be arbitrary positive integers, we define two independent families $\mathcal{G}, \mathcal{G}'$ of random vectors. \mathcal{G} has the same form as \mathcal{F} with the parameters L_0, L_1, L_2 replaced by $K_0 L_0, K_1 L_1, K_2 L_2$. \mathcal{G}' is defined analogously with the parameters on the left-hand side of (71) replaced by those on its right-hand side. Every choice of (k_0, k_1, k_2) induces a subfamily \mathcal{F} of \mathcal{G} which has the same parameters as the \mathcal{F} treated above, every subfamily of \mathcal{G}' corresponding to any (k'_0, k'_1, k'_2) induces an \mathcal{F}' with parameters L'_0, L'_1, L'_2, n' . Further recall the notation $\mathcal{G} \circ \mathcal{G}'$ as the family of concatenated words from \mathcal{G} and \mathcal{G}' .

Case 0 and 1: Let $p \in \Pi_0$ or $p \in \Pi_{H_C}^{(1)}$. Note that $\alpha_0^{(1)} \leq \alpha_1^{(1)}$ if and only if the vector $(J_0^{(\alpha)}, J_1^{(\alpha)}, J_2^{(\alpha)})$ whose components are given by

$$\begin{aligned} J_0^{(\alpha)} &= I(Z \wedge U), \\ J_1^{(\alpha)} &= \alpha I(Z \wedge X|YU) + (1 - \alpha) I(Z \wedge X|U), \\ J_2^{(\alpha)} &= \alpha I(Z \wedge Y|U) + (1 - \alpha) I(Z \wedge Y|XU) \end{aligned}$$

is contained in $\tilde{\mathcal{R}}(p)$. We first consider Case 1. Let a rate vector (R_0, R_1, R_2) with positive components be given such that $(\tilde{R}_0, \tilde{R}_1, \tilde{R}_2) := (R_0, R_1, R_2) + (J_0^{(\alpha)}, J_1^{(\alpha)}, J_2^{(\alpha)}) \in \tilde{\mathcal{R}}(p)$, which means that $(R_0, R_1, R_2) \in \mathcal{R}_\alpha(p)$. We now define a wiretap code whose rates approximate (R_0, R_1, R_2) . If $\alpha = 0$, we only need \mathcal{G}' , if $\alpha = 1$, we only need \mathcal{G} . Otherwise we do time-sharing in the following way: choose for a small $0 < \gamma < \min\{\alpha, 1 - \alpha\}$ blocklengths n and n' with $n/(n + n') \in (\alpha - \gamma, \alpha + \gamma)$. For some $0 < 2\eta < \min\{R_0, R_1, R_2\}$ and every $\nu = 0, 1, 2$ let

$$\tilde{R}_\nu - \eta \leq \frac{\log(K_\nu L_\nu) + \log(K'_\nu L'_\nu)}{n + n'} \leq \tilde{R}_\nu - \frac{\eta}{2}$$

(and this modifies accordingly for $\alpha \in \{0, 1\}$). By Lemma 4.18 we know that with probability exponentially close to 1, the random variables $\tilde{X}_{k_0 k'_0 k_1 k'_1}^{l_0 l'_0 l_1 l'_1}$ and $\tilde{Y}_{k_0 k'_0 k_2 k'_2}^{l_0 l'_0 l_2 l'_2}$ form the codewords of a code for the non-wiretap MAC given by W_b

with an average error at most $\exp(-(n+n')\zeta_1)$ for some $\zeta_1 > 0$. We denote Bob's corresponding random decoder by Φ . Now let

$$\begin{aligned}\frac{\log L_1 + \log L'_1}{n+n'} &\in J_1^{(\alpha)} + (f_1(\delta) + (\alpha f_2(\delta) + (1-\alpha)f_4(\delta))) \cdot [2, 3], \\ \frac{\log L_2 + \log L'_2}{n+n'} &\in J_2^{(\alpha)} + (f_1(\delta) + (\alpha f_4(\delta) + (1-\alpha)f_2(\delta))) \cdot [2, 3], \\ \frac{\log L_0 + \log L'_0}{n+n'} &\in J_0^{(\alpha)} + (f_4(\delta) + f_6(\delta)) \cdot [2, 3].\end{aligned}$$

This is possible if $4(f_1(\delta) + f_2(\delta) + f_4(\delta)) \leq \min\{\eta, H_C - J_0^{(\alpha)}\}$. If additionally ε is chosen according to

$$-\frac{1}{n} \log \varepsilon = \frac{1}{4} \min\{4\zeta_1, f_1(\delta) + f_2(\delta) + f_4(\delta) + f_6(\delta)\},$$

then for every $(k_0, k_1, k_2) \in [K_0] \times [K_1] \times [K_2]$, the corresponding subfamily \mathcal{F} of \mathcal{G} satisfies (33)-(36) with probability exponentially close to 1, and for every $(k'_0, k'_1, k'_2) \in [K'_0] \times [K'_1] \times [K'_2]$, the corresponding subfamily \mathcal{F}' of \mathcal{G}' satisfies (33')-(36') with probability exponentially close to 1. Thus we can choose a realization of $\mathcal{G} \circ \mathcal{G}'$ which has all these properties and use it to define a stochastic wiretap code. We define independent encoders G and G' by setting

$$\begin{aligned}G_0(l_0|k_0) &= \frac{1}{L_0}, & (k_0 \in [K_0], l_0 \in [L_0]), \\ G_1(\mathbf{x}|k_0, k_1, l_0) &= \frac{1}{L_1} \sum_{l_1} \delta_{\mathbf{x}_{k_0 l_1}^{l_0 l_1}}(\mathbf{x}), & (\mathbf{x} \in \mathcal{X}^n, k_1 \in [K_1], k_0 \in [K_0], l_0 \in [L_0]), \\ G_2(\mathbf{y}|k_0, k_2, l_0) &= \frac{1}{L_2} \sum_{l_2} \delta_{\mathbf{y}_{k_0 k_2}^{l_0 l_2}}(\mathbf{y}), & (\mathbf{y} \in \mathcal{Y}^n, k_2 \in [K_2], k_0 \in [K_0], l_0 \in [L_0]),\end{aligned}$$

and defining G' analogously. G_0 and G'_0 satisfy the common randomness constraint. We choose the decoder φ to be the realization of Φ corresponding to the chosen realization of $\mathcal{G} \circ \mathcal{G}'$. The average error of the stochastic encoding code equals the average error of the deterministic MAC code for W_b determined by the realization of $\mathcal{G} \circ \mathcal{G}'$, in particular it is bounded by ε . Due to the choice of δ the rates of this code satisfy

$$\frac{\log K_\nu + \log K'_\nu}{n+n'} \geq R_\nu - 2\eta \quad (\nu = 0, 1, 2,).$$

Finally if we let M_ν be uniformly distributed on $[K_\nu]$ and M'_ν on $[K'_\nu]$, then it follows from Lemma 4.11 and (22) together with the fact that ε is exponentially small that the strong secrecy criterion is satisfied. Thus the rate triple (R_0, R_1, R_2) is achievable. So far, this excludes (R_0, R_1, R_2) where one component equals zero, but as δ and η may be arbitrarily close to 0 and the achievable region of W is closed by definition, we can conclude that the whole region $\mathcal{R}_\alpha(p)$ is achievable.

For Case 0, everything goes through if one sets $K_0 = K'_0 = L_0 = L'_0 = 1$ and $R_0 = 0$. The difference to Case 1 is that even if $J_0^{(\alpha)} = 0$, one needs a little bit more common randomness than that in order to protect a common message, as can be seen in the choice of L_0 and L'_0 above. Thus the transmission of a common message is impossible if common randomness is not available.

Case 2: Let $p \in \Pi_{HC}^{(2)}$. In this case we generally need both a \mathcal{G} and a \mathcal{G}' , where \mathcal{G} has $L_2 = 1$ and \mathcal{G}' has $L_1 = 1$. We define the vector $(J_0^{(\alpha)}, J_1^{(\alpha)}, J_2^{(\alpha)})$ by

$$\begin{aligned} J_0^{(\alpha)} &= \alpha I(Z \wedge YU) + (1 - \alpha)I(Z \wedge XU), \\ J_1^{(\alpha)} &= \alpha I(Z \wedge X|YU), \\ J_2^{(\alpha)} &= (1 - \alpha)I(Z \wedge Y|XU) \end{aligned}$$

As it should always be clear which case we are treating, this should not lead to confusion with case 1. Note that $\alpha_0^{(2)} \leq \alpha \leq \alpha_1^{(2)}$ if and only if $(J_0^{(\alpha)}, J_1^{(\alpha)}, J_2^{(\alpha)})$ is contained in $\tilde{\mathcal{R}}(p)$ and satisfies $J_0^{(\alpha)} < H_C$. Let a rate vector (R_0, R_1, R_2) be given whose ν -th component may only vanish if $L_\nu = L'_\nu = 1$. Further we require that $(\tilde{R}_0, \tilde{R}_1, \tilde{R}_2) = (R_0, R_1, R_2) + (J_0^{(\alpha)}, J_1^{(\alpha)}, J_2^{(\alpha)})$ is contained in $\tilde{\mathcal{R}}(p)$. If $\alpha = 0$, we only need \mathcal{G}' , if $\alpha = 1$, we only need \mathcal{G} . Otherwise, let $0 < \gamma < \min\{\alpha, 1 - \alpha\}$ be small and let n and n' be large enough such that $n/(n + n') \in (\alpha - \gamma, \alpha + \gamma)$. Further for some $0 < 2\eta < \min\{R_\nu : \nu = 0, 1, 2, R_\nu > 0\}$ let

$$[\tilde{R}_\nu - \eta]_+ \leq \frac{\log(K_\nu L_\nu) + \log(K'_\nu L'_\nu)}{n + n'} \leq [\tilde{R}_\nu - \frac{\eta}{2}]_+,$$

and modify this accordingly for $\alpha \in \{0, 1\}$. By Lemma 4.18 we know that with probability exponentially close to 1, the random variables $\tilde{X}_{k_0 k'_0 k_1 k'_1}^{l_0 l'_0 l_1 l'_1}$ and $\tilde{Y}_{k_0 k'_0 k_2 k'_2}^{l_0 l'_0 l_2 l'_2}$ form the codewords of a code for the non-wiretap MAC given by W_b with an average error at most $\exp(-(n + n')\zeta_1)$ for some $\zeta_1 > 0$. We denote the corresponding random decoder by Φ . We define $(j_1^1, j_1^2) = (j_2^1, j_2^2) = (1, 2)$ and $(j_0^1, j_0^2) = (1, 6)$. Then let for $\nu = 0, 1, 2$

$$J_\nu^{(\alpha)} + 2(f_{j_\nu^1}(\delta) + f_{j_\nu^2}(\delta)) \leq \frac{\log L_\nu + \log L'_\nu}{n + n'} \leq J_\nu^{(\alpha)} + 3(f_{j_\nu^1}(\delta) + f_{j_\nu^2}(\delta)),$$

which is possible if $4(f_{j_\nu^1}(\delta) + f_{j_\nu^2}(\delta)) \leq \min\{\eta, H_C - J_0^{(\alpha)}\}$ for all ν . If additionally ε is chosen according to

$$-\frac{1}{n} \log \varepsilon = \frac{1}{4} \min\{4\zeta_1, f_1(\delta) + f_2(\delta), f_1(\delta) + f_6(\delta)\},$$

then for every $(k_0, k_1, k_2) \in [K_0] \times [K_1] \times [K_2]$, the corresponding subfamily \mathcal{F} of \mathcal{G} satisfies (53)-(55) with probability exponentially close to 1, and for every $(k'_0, k'_1, k'_2) \in [K'_0] \times [K'_1] \times [K'_2]$, the corresponding subfamily \mathcal{F}' of \mathcal{G}'

satisfies (53')-(55') with probability exponentially close to 1. Thus we can choose a realization of $\mathcal{G} \circ \mathcal{G}'$ which has all these properties plus those defining A_{MAC} and use it to define a stochastic wiretap code. We define independent encoders G and G' by setting

$$\begin{aligned} G_0(l_0|k_0) &= \frac{1}{L_0}, & (l_0 \in [L_0], k_0 \in [K_0]), \\ G_1(\mathbf{x}|k_0, k_1, l_0) &= \frac{1}{L_1} \sum_{l_1} \delta_{\mathbf{x}_{k_0 k_1}^{l_0 l_1}}(\mathbf{x}), & (\mathbf{x} \in \mathcal{X}^n, k_1 \in [K_1], k_0 \in [K_0], l_0 \in [L_0]), \\ G_2(\mathbf{y}|k_0, k_2, l_0) &= \delta_{\mathbf{y}_{k_0 k_2}^{l_0}}(\mathbf{y}), & (\mathbf{y} \in \mathcal{Y}^n, k_2 \in [K_2], k_0 \in [K_0], l_0 \in [L_0]), \end{aligned}$$

and defining G' analogously. The decoder φ is the realization of Φ corresponding to the chosen realization of $\mathcal{G} \circ \mathcal{G}'$. G_0 and G'_0 satisfy the common randomness constraint. Due to the simple form of G and G' , the average error of the stochastic encoding code equals the average error of the deterministic MAC code for W_b determined by the realization of $\mathcal{G} \circ \mathcal{G}'$, in particular it is bounded by ε . Due to the choice of δ , the rates of this code satisfy

$$\frac{\log K_\nu + \log K'_\nu}{n + n'} \geq R_\nu - 2\eta \quad (\nu = 0, 1, 2,).$$

Finally if we let M_ν be uniformly distributed on $[K_\nu]$ and M'_ν on $[K'_\nu]$, then it follows from Lemma 4.11 and (22) together with the fact that ε is exponentially small that the strong secrecy criterion is satisfied. Thus the rate triple (R_0, R_1, R_2) is achievable. So far, this may exclude rate triples (R_0, R_1, R_2) where one component equals zero, but as δ and η may be arbitrarily close to 0 and the achievable region of W is closed by definition, we can conclude that the whole region $\mathcal{R}_\alpha(p)$ is achievable.

Case 3: In this case we only need \mathcal{G} with $L_1 = L_2 = 1$. Let $R_0 > 0$ and assume that the rate vector $(\tilde{R}_0, \tilde{R}_1, \tilde{R}_2) := (R_0 + I(Z \wedge XY), R_1, R_2)$ is contained in $\tilde{\mathcal{R}}(p)$. Further for some $0 < 2\eta < \min\{R_\nu : \nu = 0, 1, 2, R_\nu > 0\}$ let

$$[\tilde{R}_\nu - \eta]_+ \leq \frac{1}{n} \log(K_\nu L_\nu) \leq [\tilde{R}_\nu - \frac{\eta}{2}]_+.$$

\mathcal{G} satisfies A_{MAC} with probability exponentially close to 1, so the $X_{k_0 k_1}^{l_0 l_1}$ and $Y_{k_0 k_2}^{l_0 l_2}$ form the codewords of a deterministic non-wiretap MAC code whose average error for transmission over W_b is bounded by $\exp(-n\zeta_1)$ for some $\zeta_1 > 0$. We denote the corresponding random decoder by Φ . Now let

$$I(Z \wedge XY) + 2(f_1(\delta) + f_2(\delta)) \leq \frac{1}{n} \log L_0 \leq I(Z \wedge XY) + 3(f_1(\delta) + f_2(\delta))$$

for δ so small that $4(f_1(\delta) + f_2(\delta)) \leq \min(\eta, H_C - I(Z \wedge XY))$ and choose ε such that

$$-\frac{1}{n} \log \varepsilon = \frac{1}{4} \min\{4\zeta_1, f_1(\delta) + f_2(\delta)\}.$$

Then for every (k_0, k_1, k_2) the corresponding family \mathcal{F} satisfies the conditions (62) and (63) with probability exponentially close to 1. We choose a realization $\{(\mathbf{u}_{k_0}^{l_0}, \mathbf{x}_{k_0 k_1}^{l_0}, \mathbf{y}_{k_0 k_2}^{l_0})\}$ which satisfies the conditions of (62) and (63) and which determines a deterministic non-wiretap code for W_b with decoder φ . Now we can define a wiretap code whose decoder is φ and whose stochastic encoder G is given by

$$\begin{aligned} G_0(l_0|k_0) &= \frac{1}{L_0}, & (k_0 \in [K_0], l_0 \in [L_0]), \\ G_1(\mathbf{x}|k_0, k_1, l_0) &= \delta_{\mathbf{x}_{k_0 k_1}^{l_0}}(\mathbf{x}), & (\mathbf{x} \in \mathcal{X}^n, k_1 \in [K_1], k_0 \in [K_0], l_0 \in [L_0]), \\ G_2(\mathbf{y}|k_0, k_2, l_0) &= \delta_{\mathbf{y}_{k_0 k_2}^{l_0}}(\mathbf{y}), & (\mathbf{y} \in \mathcal{Y}^n, k_2 \in [K_2], k_0 \in [K_0], l_0 \in [L_0]). \end{aligned}$$

Note that G_0 satisfies the common randomness constraint. Due to the uniform distribution of G_0 , its average error is identical to that of the deterministic MAC code determined by the $\mathbf{x}_{k_0 k_1}^{l_0}$ and the $\mathbf{y}_{k_0 k_2}^{l_0}$, in particular, it is exponentially small with rate at most ε . We have for $\nu = 0, 1, 2$

$$\frac{1}{n} \log K_\nu \geq R_\nu - 2\eta.$$

due to the choice of δ . Finally if we let M_ν be uniformly distributed on $[K_\nu]$, then it follows from Lemma 4.17 and (22) together with the fact that ε is exponentially small that the strong secrecy criterion is satisfied. Thus the rate triple (R_0, R_1, R_2) , and hence $\mathcal{R}(p)$, is achievable.

4.6 Concluding Steps

We can reduce coding for a general p which is the distribution of a random vector $(U, V_1, V_2, X, Y, T, Z)$ to the case treated above by constructing a new wiretap MAC as follows: its input alphabets are \mathcal{V}_1 and \mathcal{V}_2 , its output alphabets still are \mathcal{T} and \mathcal{Z} . The transition probability for inputs (v_1, v_2) and outputs (t, z) is given by

$$\tilde{W}(t, z|v_1, v_2) := \sum_{(x, y) \in \mathcal{X} \times \mathcal{Y}} W(t, z|x, y) P_{X|V_1}(x|v_1) P_{Y|V_2}(y|v_2).$$

For this channel we do the same construction as above considering the joint distribution of random variables (U, V_1, V_2, T, Z) which we denote by \tilde{p} . In this way we also construct a wiretap code for the original channel W because the additional randomness $P_{V_1 V_2|U}$ can be integrated into the stochastic encoders G_1 and G_2 . G_0 remains unchanged, so the additional randomness in the encoders does not increase the common randomness needed to do the encoding.

On the other hand, we need to show that the rate regions thus obtained are those appearing in the statement of Theorem 3.1. As the sets $\Pi_0, \Pi_{H_C}^{(1)}, \dots, \Pi_{H_C}^{(3)}$ depend on the channel, we write $\Pi_0(W), \Pi_0(\tilde{W}), \Pi_{H_C}^{(1)}(W), \dots, \Pi_{H_C}^{(3)}(\tilde{W})$. Note that \tilde{p} is contained in $\Pi_0(\tilde{W})$ or $\Pi_{H_C}^{(\nu)}(\tilde{W})$ for some $\nu = 1, 2, 3$ if and only if p is contained in the corresponding $\Pi_0(W)$ or $\Pi_{H_C}^{(\nu)}(W)$. This immediately implies that the rate regions also coincide.

5 Proof of Theorem 3.5

5.1 Elementary Rate Regions

As for the wiretap MAC with common message we show that we can write the claimed achievable regions as unions of simpler sets whose achievability will be shown in the next step.

For Case 1: Define

$$\beta_0^{(1)} := [1 - \frac{C_2}{I(Z \wedge U)}]_+, \quad \beta_1^{(1)} := \min\{\frac{C_1}{I(Z \wedge U)}, 1\}.$$

We have $\beta_0^{(1)} \leq \beta_1^{(1)}$ because $I(Z \wedge U) < C_1 + C_2$.

Lemma 5.1. *For $\beta_0^{(1)} \leq \beta \leq \beta_1^{(1)}$, let $\mathcal{R}_\beta^{(1)}(p, C_1, C_2)$ be the set of those real pairs (R_1, R_2) satisfying*

$$\begin{aligned} R_1 &\leq I(T \wedge V_1 | V_2 U) - I(Z \wedge V_1 | U) \\ &\quad - [I(Z \wedge V_2 | V_1 U) - I(T \wedge V_2 | V_1 U)]_+ - \beta I(Z \wedge U) + C_1, \\ R_2 &\leq I(T \wedge V_2 | V_1 U) - I(Z \wedge V_2 | U) \\ &\quad - [I(Z \wedge V_1 | V_2 U) - I(T \wedge V_1 | V_2 U)]_+ - (1 - \beta) I(Z \wedge U) + C_2, \\ R_1 + R_2 &\leq \min\{I(T \wedge V_1 V_2 | U) - I(Z \wedge V_1 V_2 | U) - I(Z \wedge U) + C_1 + C_2, \\ &\quad I(T \wedge V_1 V_2) - I(Z \wedge V_1 V_2)\}. \end{aligned}$$

Then

$$\mathcal{R}^{(1)}(p, C_1, C_2) = \bigcup_{\beta_0^{(1)} \leq \beta \leq \beta_1^{(1)}} \mathcal{R}_\beta^{(1)}(p, C_1, C_2).$$

Thus it is sufficient to show the achievability of $\mathcal{R}_\beta^{(1)}(p, C_1, C_2)$ for every β . For the proof one uses Lemma 4.2.

For Case 2: Recall the vector $(J_0^{(\alpha)}, J_1^{(\alpha)}, J_2^{(\alpha)})$ defined as in Case 2 from the common message part. Define

$$\beta_0^{(2, \alpha)} := [1 - \frac{C_2}{J_0^{(\alpha)}}]_+, \quad \beta_1^{(2, \alpha)} := \min\{\frac{C_1}{J_0^{(\alpha)}}, 1\}.$$

We show that every $\mathcal{R}_\alpha^{(2)}(p, C_1, C_2)$ can be represented as the union of sets $\mathcal{R}_{\alpha, \beta}^{(2)}(p, C_1, C_2)$ for $\beta_0^{(2, \alpha)} \leq \beta \leq \beta_1^{(2, \alpha)}$. Define $\mathcal{R}_{\alpha, \beta}^{(2)}(p, C_1, C_2)$ by

$$\begin{aligned} R_1 &\leq I(T \wedge V_1 | V_2 U) - \alpha I(Z \wedge V_1 | V_2 U) + C_1 - \beta J_0^{(\alpha)}, \\ R_2 &\leq I(T \wedge V_2 | V_1 U) - (1 - \alpha) I(Z \wedge V_2 | V_1 U) + C_2 - (1 - \beta) J_0^{(\alpha)}, \\ R_1 + R_2 &\leq I(T \wedge V_1 V_2 | U) - \alpha I(Z \wedge V_1 | V_2 U) - (1 - \alpha) I(Z \wedge V_2 | V_1 U) \\ &\quad + C_1 + C_2 - J_0^{(\alpha)}, \\ R_1 + R_2 &\leq I(T \wedge V_1 V_2) - I(Z \wedge V_1 V_2). \end{aligned}$$

Lemma 5.2. *We have for every $\alpha \in [\alpha_0^{(2)}, \alpha_1^{(2)}]$*

$$\mathcal{R}_\alpha^{(2)}(p, C_1, C_2) = \bigcup_{\beta_0^{(2, \alpha)} \leq \beta \leq \beta_1^{(2, \alpha)}} \mathcal{R}_{\alpha, \beta}^{(2)}(p, C_1, C_2).$$

This is seen immediately using Lemma 4.2.

For Case 3: Define

$$\beta_0^{(1)} := [1 - \frac{C_2}{I(Z \wedge V_1 V_2)}]_+, \quad \beta_1^{(1)} := \min\{\frac{C_1}{I(Z \wedge V_1 V_2)}, 1\}.$$

We have $\beta_0^{(1)} \leq \beta_1^{(1)}$ because $I(Z \wedge V_1 V_2) < C_1 + C_2$.

Lemma 5.3. *For $\beta_0^{(3)} \leq \beta \leq \beta_1^{(3)}$, let $\mathcal{R}_\beta^{(3)}(p, C_1, C_2)$ be the set of those real pairs (R_1, R_2) satisfying*

$$\begin{aligned} R_1 &\leq I(T \wedge V_1 | V_2 U_0) + C_1 - \beta I(Z \wedge V_1 V_2), \\ R_2 &\leq I(T \wedge V_2 | V_1 U_0) + C_2 - (1 - \beta) I(Z \wedge V_1 V_2), \\ R_1 + R_2 &\leq \min\{I(T \wedge V_1 V_2 | U) + C_1 + C_2 - I(Z \wedge V_1 V_2), \\ &\quad I(T \wedge V_1 V_2) - I(Z \wedge V_1 V_2)\}. \end{aligned}$$

Then

$$\mathcal{R}^{(1)}(p, C_1, C_2) = \bigcup_{\beta_0^{(1)} \leq \beta \leq \beta_1^{(1)}} \mathcal{R}_\beta^{(1)}(p, C_1, C_2).$$

Thus it is sufficient to show the achievability of $\mathcal{R}_\beta^{(3)}(p, C_1, C_2)$ for every β . For the proof one uses Lemma 4.2.

5.2 Coding

Let $C_1, C_2 > 0$ and let $p \in \Pi_{C_1+C_2}$. Further let $(R_1, R_2) \in \mathcal{R}(p, C_1, C_2)$. In Case 1 we then know that there is a $\beta \in [\beta_0^{(1)}, \beta_1^{(1)}]$ such that $(R_1, R_2) \in \mathcal{R}_\beta^{(1)}(p, C_1, C_2)$, in Case 2 we have an $\alpha \in [\alpha_0^{(2)}, \alpha_1^{(2)}]$ and a $\beta \in [\beta_0^{(2, \alpha)}, \beta_1^{(2, \alpha)}]$ with $(R_1, R_2) \in \mathcal{R}_{\alpha, \beta}^{(2)}(p, C_1, C_2)$. For Case 3, there is a $\beta \in [\beta_0^{(3)}, \beta_1^{(3)}]$ with $(R_1, R_2) \in \mathcal{R}_\beta^{(3)}(p, C_1, C_2)$. Recall the notation

$$J_0^{(\alpha)} = \begin{cases} I(Z \wedge U) & \text{in Case 1,} \\ \alpha I(Z \wedge V_2 U) + (1 - \alpha) I(Z \wedge V_1 U) & \text{in Case 2,} \\ I(Z \wedge V_1 V_2) & \text{in Case 3.} \end{cases}$$

We set

$$\tilde{R}_0^{(1)} := R_1 \wedge (C_1 - \beta J_0^{(\alpha)}), \quad \tilde{R}_0^{(2)} := R_2 \wedge (C_2 - (1 - \beta) J_0^{(\alpha)})$$

and

$$\tilde{R}_\nu := R_\nu - \tilde{R}_0^{(\nu)} \quad (\nu = 1, 2).$$

Then setting

$$\tilde{R}_0 := \tilde{R}_0^{(1)} + \tilde{R}_0^{(2)},$$

we conclude that

$$(\tilde{R}_0, \tilde{R}_1, \tilde{R}_2) \in \begin{cases} \mathcal{R}_\beta^{(1)}(p) & \text{in Case 1,} \\ \mathcal{R}_{\alpha,\beta}^{(2)}(p) & \text{in Case 2,} \\ \mathcal{R}_\beta^{(3)}(p) & \text{in Case 3.} \end{cases}$$

In particular, $(\tilde{R}_0, \tilde{R}_1, \tilde{R}_2)$ is achievable by the wiretap MAC W with common message under the common randomness bound $C_1 + C_2$. That means that for any $\eta, \varepsilon > 0$ and for sufficiently large n , there is a common-message blocklength- n code which has the form

$$\begin{aligned} \tilde{G} : [\tilde{K}_0] \times [\tilde{K}_1] \times [\tilde{K}_2] &\rightarrow \mathcal{P}(\mathcal{X}^n \times \mathcal{Y}^n), \\ \varphi : \mathcal{T}^n &\rightarrow [\tilde{K}_0] \times [\tilde{K}_1] \times [\tilde{K}_2], \end{aligned}$$

and the proof of Theorem 3.1 shows that we may assume that \tilde{G} is given by

$$\tilde{G}(\mathbf{x}, \mathbf{y} | \tilde{k}_0, \tilde{k}_1, \tilde{k}_2) = \frac{1}{\tilde{L}_0} \sum_{l_0=1}^{\tilde{L}_0} \tilde{G}_1(\mathbf{x} | \tilde{k}_0, \tilde{k}_1, l_0) \tilde{G}_2(\mathbf{y} | \tilde{k}_0, \tilde{k}_2, l_0)$$

for two stochastic matrices \tilde{G}_1, \tilde{G}_2 . For \tilde{L}_0 we have the bounds

$$J_0^{(\alpha)} + \frac{\eta}{4} \leq \frac{1}{n} \log \tilde{L}_0 \leq J_0^{(\alpha)} + \frac{\eta}{2}.$$

Without loss of generality we may additionally assume that $\tilde{L}_0^{(1)} := \tilde{L}_0^\beta$ and $\tilde{L}_0^{(2)} := \tilde{L}_0^{(1-\beta)}$ are integers. If $0 < 2\eta < \min\{\tilde{R}_\nu : \nu = 0, 1, 2, \tilde{R}_\nu > 0\}$, the codelength triple $(\tilde{K}_0, \tilde{K}_1, \tilde{K}_2)$ may be assumed to satisfy

$$[\tilde{R}_\nu - 2\eta]_+ \leq \frac{1}{n} \log \tilde{K}_\nu \leq [\tilde{R}_\nu - \eta]_+, \quad (\nu = 0, 1, 2), \quad (72)$$

and both the average error as well as $I(\tilde{M}_0 \tilde{M}_1 \tilde{M}_2 \wedge Z^n)$ are upper-bounded by ε , where $(\tilde{M}_0, \tilde{M}_1, \tilde{M}_2)$ is distributed uniformly on $[\tilde{K}_0] \times [\tilde{K}_1] \times [\tilde{K}_2]$ and Z^n is Eve's corresponding output random variable. The definitions imply that

$$\frac{1}{n} \log \tilde{K}_0 \tilde{L}_0 \leq C_1 + C_2.$$

We can find $\tilde{K}'_0, \tilde{K}_0^{(1)}, \tilde{K}_0^{(2)}$ such that $\tilde{K}'_0 = \tilde{K}_0^{(1)} \tilde{K}_0^{(2)}$ and $\tilde{K}'_0 \leq \tilde{K}_0$ and satisfying

$$[\tilde{R}_0^{(\nu)} - 2\eta]_+ \leq \frac{1}{n} \log \tilde{K}'_0 \leq [\tilde{R}_0^{(\nu)} - \frac{\eta}{2}]_+, \quad (73)$$

$$[\tilde{R}_0 - 2\eta]_+ \leq \frac{1}{n} \log \tilde{K}'_0. \quad (74)$$

Thus one obtains a natural embedding

$$[\tilde{K}_0^{(\nu)}] \times [L_0^{(\nu)}] \subset [\lfloor 2^{nC_\nu} \rfloor] \quad (\nu = 1, 2). \quad (75)$$

We now construct a wiretap code with conferencing encoders. Let

$$K_\nu := \tilde{K}_0^{(\nu)} \tilde{K}_\nu \quad (\nu = 1, 2).$$

Thus every $k_\nu \in [K_\nu]$ has the form $(a_\nu(k_\nu), b_\nu(k_\nu))$ with $a_\nu(k_\nu) \in [\tilde{K}_0^{(\nu)}]$ and $b_\nu(k_\nu) \in [\tilde{K}_\nu]$. We then define a stochastic one-shot Willems conferencing protocol

$$c_1 : [K_1] \rightarrow \mathcal{P}([\lfloor 2^{nC_1} \rfloor]), \quad c_2 : [K_2] \rightarrow \mathcal{P}([\lfloor 2^{nC_2} \rfloor])$$

which is used to generate both a common message as well as common randomness. Given a message $k_\nu \in [K_\nu]$, Alice _{ν} chooses an l_ν uniformly at random from the set $[L_0^{(\nu)}]$ and then maps the pair (k_ν, l_ν) to $(a_\nu(k_\nu), l_\nu)$, so $c_\nu(k_\nu, l_\nu) = (a_\nu(k_\nu), l_\nu)$.

Next we define stochastic encoders G_1, G_2 as in the definition of a code with conferencing encoders by setting

$$\mathcal{J} := [\lfloor 2^{nC_1} \rfloor] \times [\lfloor 2^{nC_2} \rfloor]$$

and, using the embedding (75),

$$G_1(\mathbf{x}|k_1, j) = \tilde{G}_1(\mathbf{x}|(a_1(k_1), k_0^{(2)}), b_1(k_1), (l_1, l_2))$$

if $j = ((a_1(k_1), l_1), (k_0^{(2)}, l_2))$ and letting $G_1(\mathbf{x}|k_1, j)$ be arbitrary else; G_2 is defined analogously. For decoding, one takes the decoder from the common message code and lets it combine the messages it receives into elements of $[K_1]$ and $[K_2]$. By (72), the numbers K_1 and K_2 satisfy

$$\begin{aligned} \frac{1}{n} \log K_1 &\geq R_1 - 3\eta, \\ \frac{1}{n} \log K_2 &\geq R_2 - 3\eta. \end{aligned}$$

Thus depending on the case we are in, every rate pair (R_1, R_2) contained in $\mathcal{R}_\beta^{(1)}(p, C_1, C_2)$ or $\mathcal{R}_{\alpha, \beta}^{(2)}(p, C_1, C_2)$ or $\mathcal{R}_\beta^{(3)}(p, C_1, C_2)$ is achievable.

6 Discussion

6.1 Conferencing and Secret Transmission

This subsection is devoted to the comparison of the wiretap MAC without conferencing nor common randomness and the wiretap MAC if conferencing is allowed. As our focus is on conferencing, we assume that common randomness can only be established by conferencing. We show that there exists a wiretap MAC where

the only rate pair contained in the region (10) achievable without conferencing is $(0,0)$, whereas if conferencing is enabled with arbitrarily small $C_1, C_2 > 0$, then the corresponding achievable region contains positive rates. Note that this does not mean that there are cases where conferencing is necessary to establish secret transmission as we do not have a converse. This restriction limits the use of this discussion and should be kept in mind.

Our goal is to find multiple access channels W_b and W_e such that for every Markov chain $((V_1, V_2), (X, Y), (T, Z))$ where $P_{T|XY} = W_b$ and $P_{Z|XY} = W_e$ and where V_1 and V_2 are independent one has

$$I(T \wedge V_1 V_2) \leq I(Z \wedge V_1 V_2). \quad (76)$$

We noted in Remark 3.8 that (10) is the achievable region without conferencing and it is easy to see that condition (76) is an equivalent condition for this region to equal $\{(0,0)\}$. Thus the only rate pair which is achievable according to our above considerations is $(R_1, R_2) = (0,0)$. At the same time, there should be a Markov chain $(U, (X, Y), (T, Z))$ for the same pair of channels W_b and W_e such that

$$I(T \wedge XY) > I(Z \wedge XY).$$

This would prove the existence of a rate pair (R_1, R_2) with positive components for arbitrary $C_1, C_2 > 0$.

We recall one concept of comparison for single-sender discrete memoryless channels (DMCs) introduced by Körner and Marton [22].

Definition 6.1. A DMC $W_e : \mathcal{X} \rightarrow \mathcal{P}(\mathcal{Z})$ is less noisy than a DMC $W_b : \mathcal{X} \rightarrow \mathcal{P}(\mathcal{T})$ if for every Markov chain $(U, X, (T, Z))$ with $P_{T|X} = W_b$ and $P_{Z|X} = W_e$ one has

$$I(Z \wedge U) \geq I(T \wedge U).$$

It was observed by van Dijk [35] that this is nothing but saying that the function

$$P_X \mapsto I(Z \wedge X) - I(T \wedge X), \quad P_X \in \mathcal{P}(\mathcal{X})$$

is concave. Now we generalize this to the MAC case to obtain an equivalent condition for (76).

Lemma 6.2. (76) holds for every Markov chain $((V_1, V_2), (X, Y), (T, Z))$ with independent V_1, V_2 and X independent of V_2 and Y independent of V_1 and $P_{T|XY} = W_b$ and $P_{Z|XY} = W_e$ if and only if the function

$$(P_X, P_Y) \mapsto I(Z \wedge XY) - I(T \wedge XY), \quad X, Y \text{ independent r.v.s on } \mathcal{X} \times \mathcal{Y}$$

is concave in each of its components.

Proof. Let a Markov chain be given as required in the lemma. One has

$$\begin{aligned} & I(Z \wedge V_1 V_2) - I(T \wedge V_1 V_2) \\ &= (I(Z \wedge XY) - I(T \wedge XY)) - (I(Z \wedge XY|V_1 V_2) - I(T \wedge XY|V_1 V_2)). \end{aligned} \quad (77)$$

Now note that the rightmost bracket equals

$$\sum_{v_1} \sum_{v_2} P_{V_1}(v_1) P_{V_2}(v_2) (I(Z \wedge XY | V_1 = v_1, V_2 = v_2) - I(T \wedge XY | V_1 = v_1, V_2 = v_2)),$$

so it is clear that the nonnegativity of (77) is equivalent to the concavity in each component of the function from the lemma statement. \square

We now define the channels W_b and W_e which will provide the desired example. Let N_1, N_2 be i.i.d. random variables uniformly distributed on $\{0, 1\}$. The input alphabets are $\mathcal{X} = \mathcal{Y} = \{0, 1\}$. The output alphabet of W_b is $GF(3)$ and the output alphabet of W_e is $\{-2, \dots, 3\}$. The outputs t of W_b are given by

$$t = x + y + N_1,$$

those of W_e by

$$z = 2x - 2y + N_2.$$

The intuition is that in W_e , one can exactly determine through the output whether or not the inputs were equal and if they were unequal, which input was 0 and which was 1. For W_b , however, there are for every output at least two input possibilities, so it is reasonable that an independent choice of the inputs makes W_e better than W_b . However, if one may choose the inputs with some correlation, one may choose the inputs to be equal. Then the output of W_e is only noise, whereas one can still extract some information about the input from W_b .

As the entries of the corresponding stochastic matrices of both channels are only $1/2$ or 0 , the conditional output entropy is independent of the input distribution and equals 1 . Further any pair of independent random variables on \mathcal{X} and \mathcal{Y} is given by parameters $q, r \in [0, 1]$ such that

$$\mathbb{P}[X^{(q)} = 0] = q, \quad \mathbb{P}[Y^{(r)} = 0] = r.$$

Thus in order to determine whether (76) holds, it is enough to consider the function $H(Z^{(q,r)}) - H(T^{(q,r)})$ for $T^{(q,r)}, Z^{(q,r)}$ being the outputs of W_b and W_e , respectively, corresponding to the pair $(X^{(q)}, Y^{(r)})$. One has

$$\begin{aligned} f_Z(q, r) := H(Z^{(q,r)}) &= -q(1-r) \log(q(1-r)/2) \\ &\quad - (qr + (1-q)(1-r)) \log((qr + (1-q)(1-r))/2) \\ &\quad - (1-q)r \log((1-q)r/2) \end{aligned}$$

and

$$\begin{aligned}
f_T(q, r) &:= H(T^{(q, r)}) \\
&= -\frac{1}{2}(qr + (1 - q)(1 - r)) \log((qr + (1 - q)(1 - r))/2) \\
&\quad -\frac{1}{2}(qr + q(1 - r) + (1 - q)r) \log((qr + q(1 - r) + (1 - q)r)/2) \\
&\quad -\frac{1}{2}(q(1 - r) + (1 - q)r + (1 - q)(1 - r)) \cdot \\
&\quad \cdot \log((q(1 - r) + (1 - q)r + (1 - q)(1 - r))/2).
\end{aligned}$$

Both entropies are symmetric in q and r and continuous on $[0, 1]^2$ and differentiable on $(0, 1)^2$, so by Lemma 6.2 it suffices to find the second derivatives in q of both of them and to compare.

We have

$$\begin{aligned}
\frac{\partial f_Z}{\partial q}(q, r) &= -(1 - r) \log(q(1 - r)/2) \\
&\quad - (2r - 1) \log((qr + (1 - q)(1 - r))/2) \\
&\quad + r \log((1 - q)r/2)
\end{aligned}$$

and

$$\begin{aligned}
\frac{\partial f_T}{\partial q}(q, r) &= -\frac{1}{2}(2r - 1) \log((qr + (1 - q)(1 - r))/2) \\
&\quad -\frac{1}{2}(1 - r) \log((qr + q(1 - r) + (1 - q)r)/2) \\
&\quad +\frac{r}{2} \log((q(1 - r) + (1 - q)r + (1 - q)(1 - r))/2).
\end{aligned}$$

Thus

$$\frac{\partial^2 f_Z}{\partial q^2}(q, r) = -\frac{1 - r}{q} - \frac{(2r - 1)^2}{qr + (1 - q)(1 - r)} - \frac{r}{1 - q}$$

and

$$\begin{aligned}
\frac{\partial^2 f_T}{\partial q^2}(q, r) &= -\frac{(2r - 1)^2}{2(qr + (1 - q)(1 - r))} \\
&\quad -\frac{(1 - r)^2}{2(qr + q(1 - r) + (1 - q)r)} \\
&\quad -\frac{r^2}{2(q(1 - r) + (1 - q)r + (1 - q)(1 - r))}.
\end{aligned}$$

After some algebra, it turns out that for $q, r \in (0, 1)$,

$$\begin{aligned} \frac{\partial^2 f_Z}{\partial q^2}(q, r) - \frac{\partial^2 f_T}{\partial q^2}(q, r) &= -\frac{1-r}{2q} \cdot \frac{q+2r-qr}{q+r-qr} \\ &\quad - \frac{(2r-1)^2}{2(qr+(1-q)(1-r))} \\ &\quad - \frac{r}{2(1-q)} \cdot \frac{2-r-qr}{1-qr} \\ &< 0. \end{aligned}$$

Thus $f_Z - f_T$ is concave and (76) is true for W_b, W_e .

Now we show that there exists an input distribution with $I(T \wedge XY) > I(Z \wedge XY)$. Of course, X and Y cannot be independent any more in this case. Every probability distribution p on $\{0, 1\}$ induces a probability distribution p^2 on $\{0, 1\}^2$ via $p^2(x, x) = p(x)$. Let the pair (X, Y) be distributed according to p . It is immediate from the definition of W_e that $I(Z \wedge XY) = 0$. On the other hand, P_T can be described by the vector $(1/2)(1, p(0), p(1))$. Thus one sees easily that this is maximized for $p(0) = p(1) = 1/2$, resulting in

$$I(T \wedge XY) = \frac{1}{2}.$$

p^2 is identified as an element of Π by setting $\mathcal{U} = \{0, 1\}$, $P_U = P_X$, and $P_{X|U} = P_{Y|U} = \delta_U$. Note that $I(Z \wedge U) = 0$, so secret transmission is possible with arbitrarily small conferencing capacities $C_1, C_2 > 0$.

6.2 Necessity of Time-Sharing in Random Coding

We show here that doing time-sharing during random coding is necessary for our method to work. This only serves to justify the effort we had to make in coding. We concentrate on Case 0 and 1. Then we have to show that it may happen that $\alpha_0^{(1)} > 0$ or $\alpha_1^{(1)} < 1$. Let $\mathcal{X} = \mathcal{Y} = \mathcal{T} = \mathcal{Z} = \{0, 1\}$ and let $W_b, W_e : \{0, 1\}^2 \rightarrow \mathcal{P}(\{0, 1\})$ be defined by

$$W_b = \begin{pmatrix} 0.6178 & 0.3822 \\ 0.0624 & 0.9376 \\ 0.9350 & 0.0650 \\ 0.2353 & 0.7647 \end{pmatrix}, \quad W_e = \begin{pmatrix} 0.0729 & 0.9271 \\ 0.7264 & 0.2736 \\ 0.3662 & 0.6338 \\ 0.4643 & 0.5357 \end{pmatrix},$$

where the output distribution for the input pair (x, y) is given in row number $2x + y$ for each matrix. With $q = 0.6933$ and $r = 0.3151$, let $p = p^{(q)} \otimes p^{(r)} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ be the product measure with the marginals

$$p^{(q)} = (q, 1 - q), \quad p^{(r)} = (r, 1 - r).$$

Note that $p \in \Pi_0$. One obtains the following entropies:

$$\begin{aligned} H(T|XY) &\approx 0.5685, & H(Z|XY) &\approx 0.7851, \\ H(T|X) &\approx 0.8532, & H(Z|X) &\approx 0.9952, \\ H(T|Y) &\approx 0.6251, & H(Z|Y) &\approx 0.8442, \\ H(T) &\approx 0.8866, & H(Z) &\approx 0.9999. \end{aligned}$$

Calculating with the above values returns

$$\begin{aligned} I(T \wedge XY) &= 0.3181, & I(Z \wedge XY) &= 0.2147, \\ I(T \wedge X|Y) &= 0.0566, & I(Z \wedge X|Y) &= 0.0590, \\ I(T \wedge Y|X) &= 0.2847, & I(Z \wedge Y|X) &= 0.2101, \\ & & I(Z \wedge X) &= 0.0047, \\ & & I(Z \wedge Y) &= 0.1557. \end{aligned}$$

Thus the conditions (3) and (4) are satisfied. If $H_C < \min\{I(Z \wedge X|Y), I(Z \wedge Y|X)\} = 0.0590$, then we can only show that $\mathcal{R}^{(0)}(p)$ or $\mathcal{R}^{(1)}(p)$ is achievable and might have to use time-sharing during random coding to do so. In fact, this is necessary as

$$I(Z \wedge X|Y) > I(T \wedge X|Y),$$

whereas

$$I(Z \wedge Y|X) < I(T \wedge Y|X).$$

Hence $\alpha_0^{(1)} > 0$, but $\alpha_1^{(1)} = 1$. This example was found by a brute-force search using the computer.

A Proof of Lemma 4.2

The direction “ \subset ” in (12) is obvious. For the other direction, let $(R_0, R_1, R_2) \in \mathcal{K}$. We may assume that for some $0 \leq \beta \leq 1$,

$$\begin{aligned} R_1 &= r_1 - \beta(\alpha_1 a_1 + (1 - \alpha_1)b_1) - (1 - \beta)(\alpha_0 a_1 + (1 - \alpha_0)b_1) \\ &= r_1 - (\beta\alpha_1 + (1 - \beta)\alpha_0)a_1 - (\beta(1 - \alpha_1) + (1 - \beta)(1 - \alpha_0))b_1 \end{aligned}$$

because the claim is obvious for $R_1 \leq r_1 - \alpha_1 a_1 - (1 - \alpha_1)b_1$. We show that $(R_0, R_1, R_2) \in \mathcal{K}_{\beta\alpha_1 + (1-\beta)\alpha_0}$. The R_1 -bound is satisfied due to our assumption. Further due to the bound on $R_1 + R_2$,

$$\begin{aligned} R_2 &\leq r_{12} - c - r_1 + (\beta\alpha_1 + (1 - \beta)\alpha_0)a_1 + (\beta(1 - \alpha_1) + (1 - \beta)(1 - \alpha_0))b_1 \\ &\leq r_2 - (\beta\alpha_1 + (1 - \beta)\alpha_0)a_2 - (\beta(1 - \alpha_1) + (1 - \beta)(1 - \alpha_0))b_2, \end{aligned}$$

so R_2 also satisfies the necessary upper bound. The sum constraints are independent of α . Hence all upper bounds in the definition of $\mathcal{K}_{\beta\alpha_1 + (1-\beta)\alpha_0}$ are satisfied, and Lemma 4.2 is proved.

B Proof of Lemma 4.5

For $\alpha \in [\alpha_0, \alpha_1]$, the set \mathcal{K}_α is contained in the convex hull of $\mathcal{K}_{\alpha_0} \cup \mathcal{K}_{\alpha_1}$. Thus we only have to prove that $\mathcal{K} = \text{conv}(\mathcal{K}_{\alpha_0} \cup \mathcal{K}_{\alpha_1})$. Without loss of generality we assume that $b > a$.

We first prove $\text{conv}(\mathcal{K}_{\alpha_0} \cup \mathcal{K}_{\alpha_1}) \subset \mathcal{K}$. Let $(R_0, R_1, R_2) \in \text{conv}(\mathcal{K}_{\alpha_0} \cup \mathcal{K}_{\alpha_1})$. Using the convexity of \mathcal{K}_{α_0} and \mathcal{K}_{α_1} we infer that there is a $(R_0^{(0)}, R_1^{(0)}, R_2^{(0)}) \in \mathcal{K}_{\alpha_0}$ and a $(R_0^{(1)}, R_1^{(1)}, R_2^{(1)}) \in \mathcal{K}_{\alpha_1}$ and a $\beta \in [0, 1]$ such that

$$(R_0, R_1, R_2) = \beta(R_0^{(0)}, R_1^{(0)}, R_2^{(0)}) + (1 - \beta)(R_0^{(1)}, R_1^{(1)}, R_2^{(1)}).$$

One sees immediately that (R_0, R_1, R_2) satisfies the bounds (17)-(19) and (21). It is sufficient to check that (20) is satisfied by the triples $(R_0^{(0)}, R_1^{(0)}, R_2^{(0)})$ and $(R_0^{(1)}, R_1^{(1)}, R_2^{(1)})$. For $(R_0^{(0)}, R_1^{(0)}, R_2^{(0)})$ we assume that

$$R_1^{(0)} = \gamma(r_1 - \alpha_0 a)$$

for some $\gamma \in [0, 1]$. After some calculations this yields

$$\begin{aligned} bR_1^{(0)} + aR_2^{(0)} &\leq (b - a)r_1 + ar_{12} - ab - (1 - \gamma)(b - a)(r_1 - \alpha_0 a) \\ &\leq (b - a)r_1 + ar_{12} - ab. \end{aligned}$$

One proceeds analogously for $(R_0^{(1)}, R_1^{(1)}, R_2^{(1)})$.

Next we have to check that $\mathcal{K} \subset \text{conv}(\mathcal{K}_{\alpha_0} \cup \mathcal{K}_{\alpha_1})$. It is sufficient to check whether those points (R_0, R_1, R_2) are contained in $\text{conv}(\mathcal{K}_{\alpha_0} \cup \mathcal{K}_{\alpha_1})$ that satisfy both (20) and one of (17)-(19) with equality. So assume that

$$bR_1 + aR_2 = r_{12}a + r_1(b - a) - ab. \quad (78)$$

First we also assume that

$$R_1 + R_2 = r_{12} - \alpha_0 a - (1 - \alpha_1)b.$$

Then

$$R_2 = r_{12} - \alpha_0 a - (1 - \alpha_1)b - R_1$$

and using (78) we obtain

$$R_1 = r_1 - \frac{\alpha_1 b - \alpha_0 a}{b - a} a \leq r_1 - \alpha_1 a.$$

For R_2 this gives

$$R_2 = r_{12} - r_1 - \left(\alpha_0 + \frac{\alpha_1 b - \alpha_0 a}{b - a} \right) a - (1 - \alpha_1)b \leq r_2 - (1 - \alpha_1)b,$$

so $(R_1, R_2) \in \mathcal{K}_{\alpha_1}$.

Now we assume

$$R_1 = r_1 - \alpha_0 a.$$

Then inserting this in (78) one obtains

$$R_2 \leq r_2 - (1 - \alpha_0)b,$$

so $(R_1, R_2) \in \mathcal{K}_{\alpha_0}$.

Finally for

$$R_2 = r_2 - (1 - \alpha_1)b$$

we obtain

$$R_1 \leq r_1 - \alpha_1 a,$$

so $(R_1, R_2) \in \mathcal{K}_{\alpha_1}$. This proves the lemma.

References

1. Ahlswede, R.: Elimination of correlation in random codes for arbitrarily varying channels. *Z. Wahrscheinlichkeitstheorie verw. Gebiete* **44** (1978) 159–175
2. Ahlswede, R.: Coloring hypergraphs: A new approach to multi-user source coding—II. *J. Comb. Inform. Syst. Sci.* **5**(3) (1980) 220–268
3. Ahlswede, R.: Arbitrarily varying channels with states sequence known to the sender. *IEEE Trans. Inf. Theory* **IT-32**(5) (1986) 621–629
4. Ahlswede, R.: On concepts of performance parameters for channels. Ahlswede, Rudolf (ed.) et al., *General theory of information transfer and combinatorics*. Berlin: Springer. *Lecture Notes in Computer Science* 4123, 639–663 (2006). (2006)
5. Ahlswede, R., Cai, N.: Arbitrarily varying multiple-access channels part I—Ericson’s symmetrizability is adequate, Gubner’s conjecture is true. *IEEE Trans. Inf. Theory* **45**(2) (1999) 742–749
6. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography—part I: Secret sharing. *IEEE Trans. Inf. Theory* **39**(4) (1993)
7. Ahlswede, R., Csiszár, I.: Common randomness in information theory and cryptography—part II: CR capacity. *IEEE Trans. Inf. Theory* **44**(1) (1998)
8. Ahlswede, R., Winter, A.: Strong converse for identification via quantum channels. *IEEE Trans. Inf. Theory* **48**(3) (2002) 569–579
9. Ahlswede, R.: Multi-way communication channels. In: *Proceedings of 2nd International Symposium on Information Theory*, Tsahkadsor, Armenian SSR, Akadémiai Kiadó, Budapest (1971) 23–52
10. Ahlswede, R.: An elementary proof of the strong converse theorem for the multiple-access channel. *J. Comb. Inf. Syst. Sci.* **7** (1982) 216–230
11. Bjelaković, I., Boche, H., Sommerfeld, J.: Secrecy results for compound wiretap channels. available online at <http://arxiv.org/abs/1106.2013> (2011)
12. Bloch, M.R., Laneman, J.N.: Secrecy from resolvability. Submitted to *IEEE Trans. Inf. Theory* (May 2011)
13. Cai, N., Winter, A., Yeung, R.W.: Quantum privacy and quantum wiretap channels. *Problems of Information Transmission* **40**(4) (2004) 318–336
14. Csiszár, I.: Almost independence and secrecy capacity. *Problems of Information Transmission* **32**(1) (1996) 40–47

15. Csiszár, I., Körner, J.: Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **IT-24**(3) (1978) 339–348
16. Csiszár, I., Körner, J.: *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Second edn. Cambridge University Press, Cambridge (2011)
17. Devetak, I.: The private classical capacity and quantum capacity of a quantum channel. *IEEE Trans. Inf. Theory* **51**(1) (2005) 44–55
18. Dueck, G.: The strong converse of the coding theorem for the multiple-access channel. *J. Comb. Inf. Syst. Sci.* **6** (1981) 187–196
19. Ekrem, E., Ulukus, S.: Effects of cooperation on the secrecy of multiple access channels with generalized feedback. In: *Proc. Conf. on Inf. Sciences and Systems (CISS)*, Princeton, NJ (March 2008) 791–796
20. Ekrem, E., Ulukus, S.: On the secrecy of multiple access wiretap channel. In: *Proc. Allerton Conference*, Allerton House, UIUC, IL, USA (September 2008) 1014–1021
21. He, X., Yener, A.: MIMO wiretap channel with arbitrarily varying eavesdropper channel states. submitted to *IEEE Trans. Inf. Theory*, available at <http://arxiv.org/abs/1007.4801> (2010)
22. Körner, J., Marton, K.: The comparison of two noisy channels. In Csiszár, I., Elias, P., eds.: *Topics in Information Theory*. Number 16 in *Coll. Math. Soc. J. Bolyai*. North Holland, Amsterdam (1977)
23. Liang, Y., Poor, H.V.: Multiple-access channels with confidential messages. *IEEE Trans. Inf. Theory* **54**(3) (2008) 976–1002
24. Liang, Y., Poor, H.V., Shamai, S.: Information theoretic security. *Found. Trends Commun. Inf. Theory* **5**(4-5) (2008) 355–580
25. Liao, H.J.: *Multiple Access Channels*. PhD thesis, Dept. of Electrical Engineering, University of Hawaii, Honolulu (1972)
26. Liu, R., Liang, Y., Poor, H.V.: Fading cognitive multiple-access channels with confidential messages. Submitted to *IEEE Trans. Inf. Theory*, available at <http://arxiv.org/abs/0910.4613> (2009)
27. Liu, R., Marić, I., Yates, R., Spasojević, P.: The discrete memoryless multiple-access channel with confidential messages. In: *Proc. Int. Symp. Inf. Theory*, Seattle, USA (July 2006) 957–961
28. Maurer, U.M.: Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory* **39**(3) (1993) 733–742
29. Maurer, U.: The strong secret key rate of discrete random triples. In Blahut, R., ed.: *Communication and Cryptography — Two Sides of One Tapestry*. Kluwer Academic Publishers (1994) 271–285
30. Pierrot, A.J., Bloch, M.R.: Strongly secure communications over the two-way wiretap channel. *IEEE Trans. Inf. Forensics Secur.* **6**(3)
31. Simeone, O., Yener, A.: The cognitive multiple access wire-tap channel. In: *Proc. Conf. on Inf. Sciences and Systems (CISS)*, Baltimore, NJ, USA (March 2009)
32. Slepian, D., Wolf, K.: A coding theorem for multiple access channels with correlated sources. *Bell Sytem Techn. J.* **52**(7) (1973) 1037–1076
33. Tang, X., Liu, R., Spasojević, P., Poor, H.V.: Multiple access channels with generalized feedback and confidential messages. In: *Proc. Inf. Theory Workshop*, Lake Tahoe, CA, USA (September 2007) 608–613
34. Tekin, E., Yener, A.: The gaussian multiple access wire-tap channel. *IEEE Trans. Inf. Theory* **54**(12) (2008) 5747–5755
35. van Dijk, M.: On a special class of broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **43**(2) (1997) 712–714

36. Wiese, M., Boche, H.: The arbitrarily varying multiple-access channel with conferencing encoders. Submitted to IEEE Trans. Inf. Theory, available at <http://arxiv.org/abs/1105.0319> (2011)
37. Wiese, M., Boche, H., Bjelaković, I., Jungnickel, V.: The compound multiple access channel with partially cooperating encoders. IEEE Trans. Inf. Theory **57**(5) (2011) 3045–3066
38. Willems, F.M.J.: Informationtheoretical Results for the Discrete Memoryless Multiple Access Channel. PhD thesis, Katholieke Universiteit Leuven, Belgium (1982)
39. Willems, F.M.J.: The discrete memoryless multiple access channel with partially cooperating encoders. IEEE Trans. Inf. Theory **IT-29**(3) (1983) 441–445
40. Wyner, A.: The wire-tap channel. The Bell System Tech. J. **54**(8) (1975) 1355–1387
41. Wyrembelski, R.F., Wiese, M., Boche, H.: Strong secrecy in bidirectional relay networks. In: Proc. Asilomar Conference on Signals, Systems and Computers (ACSSC '11), Pacific Grove, CA, USA (November 2011)
42. Yassaee, M.H., Aref, M.R.: Multiple access wiretap channels with strong secrecy. In: Proc. IEEE Information Theory Workshop (ITW 2010), Dublin, Ireland (August/September 2010)